

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

20 novembre 2023

PROJET DE LOI

portant création de la banque de données commune “Terrorisme, Extrémisme, processus de Radicalisation” (“T.E.R.”) et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d’extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police

Sommaire Pages

Résumé	3
Exposé des motifs	4
Avant-projet de loi	160
Avis du Conseil d’État	187
Projet de loi	224
Coordination des articles	267
Avis de l’Autorité de protection des données	341
Avis de l’Organe de Contrôle de l’Information policière	429

CONFORMÉMENT À L’ARTICLE 8, § 2, 1°, DE LA LOI DU 15 DÉCEMBRE 2013, L’ANALYSE D’IMPACT N’A PAS ÉTÉ DEMANDÉE.

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

20 november 2023

WETSONTWERP

tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”) en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt

Inhoud Blz.

Samenvatting	3
Memorie van toelichting	4
Voorontwerp van wet	160
Advies van de Raad van State	187
Wetsontwerp	224
Coördinatie van de artikelen	303
Advies van de Gegevensbeschermingsautoriteit	384
Advies van het Controleorgaan op de politionele informatie	442

OVEREENKOMSTIG ARTIKEL 8, § 2, 1°, VAN DE WET VAN 15 DECEMBER 2013 WERD DE IMPACTANALYSE NIET GEVRAAGD.

Le gouvernement a déposé ce projet de loi le 20 novembre 2023.

Le “bon à tirer” a été reçu à la Chambre le 22 novembre 2023.

De regering heeft dit wetsontwerp op 20 november 2023 ingediend.

De “goedkeuring tot drukken” werd op 22 november 2023 door de Kamer ontvangen.

N-VA	: Nieuw-Vlaamse Alliantie
Ecolo-Groen	: Ecologistes Confédérés pour l'organisation de luttes originales – Groen
PS	: Parti Socialiste
VB	: Vlaams Belang
MR	: Mouvement Réformateur
cd&v	: Christen-Democratisch en Vlaams
PVDA-PTB	: Partij van de Arbeid van België – Parti du Travail de Belgique
Open Vld	: Open Vlaamse liberalen en democraten
Vooruit	: Vooruit
Les Engagés	: Les Engagés
DéFI	: Démocrate Fédéraliste Indépendant
INDEP-ONAFH	: Indépendant - Onafhankelijk

Abréviations dans la numérotation des publications:		Afkorting bij de nummering van de publicaties:	
DOC 55 0000/000	Document de la 55 ^e législature, suivi du numéro de base et numéro de suivi	DOC 55 0000/000	Parlementair document van de 55 ^e zittingsperiode + basisnummer en volgnummer
QRVA	Questions et Réponses écrites	QRVA	Schriftelijke Vragen en Antwoorden
CRIV	Version provisoire du Compte Rendu Intégral	CRIV	Voorlopige versie van het Integraal Verslag
CRABV	Compte Rendu Analytique	CRABV	Beknopt Verslag
CRIV	Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)	CRIV	Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)
PLEN	Séance plénière	PLEN	Plenum
COM	Réunion de commission	COM	Commissievergadering
MOT	Motions déposées en conclusion d'interpellations (papier beige)	MOT	Moties tot besluit van interpellaties (beigegekleurig papier)

RÉSUMÉ

Le présent projet de loi vise à transposer dans une loi autonome les dispositions de la loi du 5 août 1992 sur la fonction de police relatives aux banques de données communes “Terrorist fighters” et “Propagandistes de haine”, dont les modalités de traitement sont détaillées dans l’arrêté royal du 21 juillet 2016 relatif à la banque de données commune “Terrorist Fighters” et dans l’arrêté royal du 23 avril 2018 relatif à la banque de données commune “Propagandistes de haine” et portant exécution de certaines dispositions de la section 1^{re} bis “de la gestion des informations” du chapitre IV de la loi sur la fonction de police.

Ce faisant, il entérine le fait qu’il n’y a qu’une seule banque de données commune pour traiter les matières de terrorisme, d’extrémisme et de radicalisme pour les services de base, les services partenaire et le parquet (la BDC T.E.R.).

Le projet de loi énumère les différents services de base et partenaires et spécifie les différentes typologies des droits d’utilisation de la banque de données commune T.E.R.: droit de créer, droit de lire, droit d’écrire, droit d’interrogation et droit d’accès aux archives.

En outre, le projet de loi intègre dans la loi les différentes catégories de personnes traitées dans la BDC T.E.R., alors qu’auparavant celles-ci étaient énumérées dans un arrêté royal. Ces catégories sont les suivantes: Les Foreign Terrorist Fighters, les Homegrown Terrorist Fighter, les Extrémistes Potentiellement Violents, les Propagandistes de Haine et les Condamnés pour Terrorisme. Afin de fournir une base juridique pour la discussion et l’enquête sur les personnes qui pourraient avoir besoin d’un statut à part entière dans la BDC T.E.R., ce projet prévoit également une catégorie d’Enquête Préliminaire.

Le projet prévoit désormais que la BDC T.E.R. peut être interconnectée avec une autre banque de données “opérationnelle” d’un service de base ou d’un service partenaire ou avec une source authentique.

Le projet ajoute des dispositions supplémentaires pour mettre la réglementation actuelle en conformité avec les règles en matière de protection des données à caractère personnel.

Enfin, ce projet confirme l’existence des Task Forces Locales et détermine ses missions.

SAMENVATTING

Dit wetsontwerp strekt tot de opname in een autonome wet van de bepalingen van de wet van 5 augustus 1992 op het politieambt met betrekking tot de gemeenschappelijke gegevensbanken “Terrorist Fighters” en “Haatpropagandisten”, waarvan de verwerkingsmodaliteiten worden uiteengezet in het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Terrorist Fighters en in het koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1bis “Het informatiebeheer” van hoofdstuk IV van de wet op het politieambt.

Op die manier bekrachtigt de wet het feit dat er slechts één gemeenschappelijke gegevensbank bestaat voor de behandeling van terrorisme, extremisme en radicalisme voor de basisdiensten, de partnerdiensten en het parket (de GGB T.E.R.).

Het wetsontwerp somt de verschillende basisdiensten en partnerdiensten op en specificeert de verschillende soorten gebruiksrechten voor de gemeenschappelijke T.E.R.-databank: het recht om te creëren, het recht om te lezen, het recht om te schrijven, de rechtstreekse bevraging en het recht op toegang tot de archieven.

Hiernaast neemt het wetsontwerp de verschillende categorieën van personen van de GGB T.E.R. op in de wet, waar dit eerder in een koninklijk besluit werd bepaald. De categorieën zijn: Foreign Terrorist Fighters, Homegrown Terrorist Fighter, Potentieel Gewelddadig Extremist, Haatpropagandist en Terrorisme Veroordeelde. Om een wettelijke basis te geven aan de bespreking en onderzoek van personen die mogelijk een volwaardig statuut in de GGB T.E.R. moeten krijgen, wordt in dit ontwerp ook een categorie Vooronderzoek voorzien.

Het ontwerp voorziet verder dat de GGB T.E.R. gekoppeld kan worden aan een andere “operationele” database van een basisdienst of partnerdienst, of aan een authentieke bron.

In het ontwerp worden nog bepalingen toegevoegd om de huidige regelgeving in lijn te brengen met de bescherming van persoonsgegevens.

Tot slot bevestigt dit ontwerp het bestaan van de Lokale Taskforces en legt het de opdrachten ervan vast.

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

EXPOSÉ GÉNÉRAL

1. Généralités

MESDAMES, MESSIEURS,

La loi du 27 avril 2016 relative à des mesures complémentaires en matière de lutte contre le terrorisme prévoit, au sein de la section 1bis “De la gestion des informations” du chapitre IV de la loi sur la fonction de police, la possibilité pour les ministres de l’Intérieur et de la Justice de créer des banques de données communes.

Ces banques de données communes permettent à différents services ayant des compétences différentes mais poursuivant le même objectif de prévenir et lutter contre le terrorisme et l’extrémisme pouvant mener au terrorisme, de partager leurs données et informations afin d’être plus efficaces dans ce cadre.

Vu l’objectif ci-dessus, et en raison du départ d’un certain nombre de ressortissants belges vers les zones de conflits irako-syriennes, et plus particulièrement à la suite des attentats de Paris en 2015 et de Bruxelles en 2016, la banque de données commune “*Foreign terrorist fighters*” a été créée par l’arrêté royal du 21 juillet 2016 (*Moniteur belge* du 22 septembre 2016) (ci-après, arrêté royal “TF”). Cette banque de données avait pour but de contribuer à l’analyse, à l’évaluation et au suivi des *foreign terrorist fighters* et du phénomène sur base d’une évaluation de la menace.

En 2018, par l’arrêté royal du 23 avril 2018 modifiant l’arrêté royal du 21 juillet 2016, la banque de données commune “*Foreign Terrorist Fighters*” devient la banque de données commune “*Terrorist Fighters*”. La banque de données commune a ainsi été modifiée au niveau d’une part, de sa dénomination et d’autre part, des données qui y sont traitées pour y inclure une nouvelle catégorie de personnes physiques: les *Homegrown Terrorist Fighters*.

Un second arrêté royal adopté à la même date crée la banque de données commune “*Propagandiste de haine*” (ci-après, arrêté royal “PH”). Cette banque de données commune s’inscrit dans la lutte contre le terrorisme et se concentre plus particulièrement sur l’influence

MEMORIE VAN TOELICHTING

DAMES EN HEREN,

ALGEMENE TOELICHTING

1. Algemeen

DAMES EN HEREN,

De wet van 27 april 2016 inzake aanvullende maatregelen ter bestrijding van terrorisme voorziet in afdeling 1bis “Het informatiebeheer” van hoofdstuk IV van de wet op het politieambt in de mogelijkheid voor de ministers van Binnenlandse Zaken en van Justitie om gemeenschappelijke gegevensbanken op te richten.

Aan de hand van deze gemeenschappelijke gegevensbanken kunnen verscheidene diensten met verschillende bevoegdheden maar met dezelfde doelstelling inzake het voorkomen en bestrijden van terrorisme en extremisme dat tot terrorisme kan leiden, hun gegevens en informatie delen teneinde in dit kader doeltreffender te zijn.

Gelet op de bovenstaande doelstelling en op het gegeven dat een aantal Belgische onderdanen naar Iraaks-Syrische conflictzones waren afgereisd, en meer in het bijzonder ingevolge de aanslagen in Parijs van 2015 en de aanslagen in Brussel van 2016, werd de gemeenschappelijke gegevensbank “*Foreign Terrorist Fighters*” opgericht bij het koninklijk besluit van 21 juli 2016 (*Belgisch Staatsblad* van 22 september 2016) (hierna koninklijk besluit “TF”). Het doel van deze gegevensbank was om bij te dragen tot de analyse, de evaluatie en de opvolging van *foreign terrorist fighters* en van het fenomeen op basis van een evaluatie van de dreiging.

In 2018, bij het koninklijk besluit van 23 april 2018 tot wijziging van het koninklijk besluit van 21 juli 2016, werd de gemeenschappelijke gegevensbank “*Foreign Terrorist Fighters*” omgevormd tot de gemeenschappelijke gegevensbank “*Terrorist Fighters*”. Aldus werd de gemeenschappelijke gegevensbank gewijzigd, zowel wat de naam als wat de erin verwerkte gegevens betreft, door een nieuwe categorie natuurlijke personen toe te voegen, namelijk de *Homegrown Terrorist Fighters*.

Een tweede koninklijk besluit dat op dezelfde datum werd goedgekeurd, voorzag in de oprichting van de gemeenschappelijke gegevensbank “*Haatpropagandisten*” (hierna koninklijk besluit “HP”). Deze gemeenschappelijke gegevensbank kadert in de strijd tegen het terrorisme

radicalisante qui est souvent à la base du passage au terrorisme ou à l'extrémisme pouvant mener au terrorisme.

Enfin, l'arrêté royal du 20 décembre 2019 apporte des modifications techniques aux arrêtés royaux précités et ajoutent deux catégories supplémentaires de personnes dans la banque de données commune "*Terrorist fighters*", à savoir les "Extrémistes Potentiellement Violents" et les "Personnes condamnées pour terrorisme".

Il convient ici de clarifier un point important: contrairement à ce qu'indique l'Organe de contrôle de l'information policière (C.O.C.) et le Comité permanent R dans leur rapport 2020, la banque de donnée commune "Propagandiste de haine" ne constitue pas une banque de donnée commune distincte de la banque de donnée commune "*Terrorist fighters*". En effet, techniquement, il n'existe qu'une seule banque de données commune, laquelle comprend les différentes catégories de personnes ou entités listées dans l'arrêté royal du 21 juillet 2016 et dans l'arrêté royal du 23 avril 2018 précités. Le rapport au Roi de l'arrêté royal du 20 décembre 2019 précité confirme d'ailleurs que "Fondamentalement, il s'agit d'une seule banque de données, articulée autour des différentes catégories de personnes qui peuvent y être traitées."

Le présent projet de loi vise à transposer dans une loi autonome les dispositions de la loi sur la fonction de police relatives aux banques de données communes "*Terrorist fighters*" et "Propagandistes de haine", créées par l'arrêté royal du 21 juillet 2016 relatif à la banque de données commune "*Terrorist Fighters*" et par l'arrêté royal du 23 avril 2018 relatif à la banque de données commune "Propagandistes de haine".

La création d'une loi autonome pour la banque de données commune en matière de terrorisme, extrémisme ou processus de radicalisation est motivée par les raisons exposées ci-dessous:

Il s'agissait tout d'abord de répondre à une demande émanant tant de la Commission d'enquête parlementaire que de l'Autorité de protection des données visant à donner une base juridique ad hoc à cette banque de données, qui comme son nom l'indique, est commune à différents services et qui n'avait donc pas de raison spécifique d'être attachée à la loi sur la fonction de police.

D'une part, dans son troisième rapport intermédiaire sur le volet "architecture de la sécurité", la Commission d'enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes

en focust meer bepaald op de radicaliserende invloed die vaak ten grondslag ligt aan de overgang naar terrorisme of van extremisme dat kan leiden tot terrorisme.

Tot slot brengt het koninklijk besluit van 20 december 2019 technische wijzigingen aan in de voornoemde koninklijke besluiten en voegt het twee aanvullende categorieën van personen toe aan de gemeenschappelijke gegevensbank "*Terrorist fighters*", namelijk de "Potentieel Gewelddadige Extremisten" en de "Terrorisme-veroordeelden".

Hier moet een belangrijk punt verduidelijkt worden: in tegenstelling tot wat het Controleorgaan op de Politie Informatie (COC) en het Vast Comité I in hun verslag van 2020 aangeven, staat de gemeenschappelijke gegevensbank "Haatpropagandisten" niet los van de gemeenschappelijke gegevensbank "*Terrorist Fighters*". Vanuit technisch oogpunt bestaat er namelijk slechts één gemeenschappelijke gegevensbank, die de verschillende categorieën van personen of entiteiten bevat die opgesomd worden in de voornoemde koninklijke besluiten van 21 juli 2016 en 23 april 2018. Dat wordt trouwens ook bevestigd in het verslag aan de Koning bij het voornoemde koninklijk besluit van 20 december 2019: "In principe gaat het om één enkele gegevensbank die ingedeeld is in verschillende categorieën van personen die in de gegevensbank verwerkt kunnen worden."

Dit wetsontwerp strekt tot de omzetting in een autonome wet van de bepalingen in de wet op het politieambt met betrekking tot de gemeenschappelijke gegevensbanken "*Terrorist Fighters*" en "Haatpropagandisten", opgericht bij het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank *Terrorist Fighters* en het koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten.

De oprichting van een autonome wet voor de gemeenschappelijke gegevensbank inzake terrorisme, extremisme of het radicaliseringsproces wordt gemotiveerd om de hieronder uiteengezette redenen:

Eerst en vooral ging het erom gehoor te geven aan een verzoek vanwege zowel de parlementaire onderzoekscommissie als de Gegevensbeschermingsautoriteit om een ad hoc rechtsgrondslag te geven aan deze gegevensbank, die – zoals zijn naam aangeeft – voor verschillende diensten gemeenschappelijk is en dus geen specifieke reden had om aan de wet op het politieambt te zijn gekoppeld.

Eenzijds, in haar derde tussentijdse verslag over het onderdeel "veiligheidsarchitectuur" heeft de parlementaire onderzoekscommissie belast met het onderzoek naar de omstandigheden die hebben geleid tot de terroristische

du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre la radicalisation et la menace terroriste, a émis un certain nombre de recommandations concernant la banque de données commune "*Foreign terrorist fighters*". Elle constate, entre autres, que l'extension de la loi sur la fonction de police ne constitue pas une base adéquate pour la création de banques de données d'une telle importance. (DOC 54 1752/008, p. 233).

D'autre part, la Commission de protection de la vie privée, devenue l'Autorité de protection des données, a fait le même constat dans son avis n° 57/2015 du 16 décembre 2015 (considérant 23).

Ensuite en 2021, l'affaire Conings, concernant un militaire ayant une idéologie d'extrême droite et suspecté d'avoir voulu perpétrer une attaque terroriste, a relancé le débat au sujet des conséquences d'une inscription d'un individu dans la banque de données commune "*Terrorist fighters*" et a entraîné une volonté de modifier la législation concernant la banque de données commune à ce sujet. Ce militaire avait, en effet, emporté des armes et des munitions de la caserne où il officiait en utilisant les accès dont il disposait toujours malgré son inscription dans la banque de données commune T.E.R. C'est pour répondre à ce point que le chapitre 3 a été ajouté et prévoit dorénavant l'obligation pour la Task Force Locale, lorsqu'une entité est reprise dans la banque de données commune T.E.R. de parcourir une liste de mesures qui peuvent être prises à l'égard d'une entité.

Enfin, par suite du décès tragique d'un policier poignardé par une personne enregistrée dans la banque de données T.E.R. et qui avait été conduite dans un hôpital suite à la suspicion de troubles psychiatriques mais qui est repartie avant d'avoir été examinée par un professionnel de la santé, il est apparu nécessaire d'une part, de permettre aux services de base de communiquer des données relatives à la santé mentale et physique et à la dangerosité des personnes enregistrées dans la banque de données T.E.R. aux professionnels des soins de santé. Il est aussi apparu d'autre part, nécessaire de prévoir une procédure afin de permettre à l'ensemble des policiers qui sont sur le terrain de pouvoir prendre connaissance de l'évaluation de la menace d'une personne qui est enregistrée dans la banque de données T.E.R. et avec laquelle ils sont en contact sans devoir disposer d'une habilitation de sécurité.

aanslagen van 22 maart 2016 in de luchthaven Brussel-Nationaal en in het metrostation Maalbeek te Brussel, met inbegrip van de evolutie en de aanpak van de strijd tegen het radicalisme en de terroristische dreiging, een aantal aanbevelingen geformuleerd met betrekking tot de gemeenschappelijke gegevensbank "*Foreign Terrorist Fighters*". Ze stelt onder meer vast dat het uitbreiden van de wet op het politieambt geen adequate basis is voor de oprichting van dergelijke belangrijke gegevensbanken (DOC 54 1752/008, blz. 233).

Anderzijds, heeft de Commissie voor de bescherming van de persoonlijke levenssfeer, die de Gegevensbeschermingsautoriteit is geworden, hetzelfde vastgesteld in haar advies nr. 57/2015 van 16 december 2015 (overweging 23).

Vervolgens heeft in 2021 de zaak Conings, betreffende een militair die er een rechts-extremistische ideologie op nahield en die ervan werd verdacht een terroristische aanslag te willen plegen, het debat over de gevolgen van de inschrijving van een individu in de gemeenschappelijke gegevensbank "*Terrorist Fighters*" weer op gang gebracht en heeft het geleid tot de bereidheid om de wetgeving betreffende de gemeenschappelijke gegevensbank op dit gebied te wijzigen. Die militair had namelijk wapens en munitie meegenomen uit de kazerne waar hij werkzaam was door gebruik te maken van de toegang waarover hij nog steeds beschikte ondanks dat hij ingeschreven stond in de gemeenschappelijke gegevensbank T.E.R. Om aan dat punt tegemoet te komen werd hoofdstuk 3 toegevoegd, waarin voortaan wordt voorzien in de verplichting voor de Lokale Taskforce om, wanneer er een entiteit in de gemeenschappelijke gegevensbank T.E.R. wordt opgenomen, een lijst maatregelen te overlopen die ten aanzien ervan kunnen worden genomen.

Tot slot, als gevolg van het tragische overlijden van een politieagent die werd neergestoken door een persoon die in de gegevensbank T.E.R. was opgenomen en naar een ziekenhuis was gevoerd naar aanleiding van een vermoedelijke psychiatrische stoornis, maar die was vertrokken vooraleer hij door een zorgverlener werd onderzocht, is het noodzakelijk gebleken om de basisdiensten de mogelijkheid te bieden gegevens inzake mentale en fysieke gezondheid en inzake de gevaarlijkheid van personen opgenomen in de gegevensbank T.E.R. mee te delen aan zorgverleners. Het is daarnaast noodzakelijk gebleken te voorzien in een procedure om ervoor te zorgen dat alle politieagenten in het veld kennis kunnen nemen van de evaluatie van de dreiging van een persoon die in de gegevensbank T.E.R. is opgenomen en met wie ze in contact komen, zonder dat ze daarvoor over een veiligheidsmachtiging hoeven te beschikken.

2. Objectif du projet

Le projet a pour objectif d'une part, de transposer dans une loi spécifique les dispositions de la loi sur la fonction de police relatives à la banque de données commune "Terrorist fighters" et "Propagandistes de haine" et d'autre part, de renforcer la stratégie T.E.R relative à la banque de données commune et aux Task Forces locales. Ce renforcement est mis en œuvre de différentes manières. Il s'agit tout d'abord de simplifier cette législation et de la rendre plus lisible. Pour ce faire, certaines dispositions existantes ont été retravaillées, tant au niveau de leur libellé que de leur structure. Ensuite, un maximum d'éléments contenus dans les arrêtés royaux d'exécution sont intégrés dans la loi pour donner une assise juridique plus forte à certaines dispositions, notamment en matière de protection des personnes à l'égard de traitements de données à caractère personnel et au niveau des catégories de données traitées. L'objectif est aussi, dans le cadre de la stratégie T.E.R., de mettre l'accent sur la nécessaire concertation entre professionnels de la sécurité à propos des données contenues dans la banque de données commune T.E.R. lesquels doivent notamment s'entendre sur l'opportunité de la prise de mesures lorsqu'une entité est enregistrée dans la banque de données commune.

Il faut noter que la majorité des articles de la loi sur la fonction de police ou des arrêtés royaux "TF" et "PH" existants a été transférée dans le présent projet sans modification de fond. Dans la mesure où le projet maintient, *de facto*, le dispositif existant, les justifications qui sous-tendaient l'adoption de ces dispositions restent dès lors d'application et ne sont pas reprises de nouveau dans cet exposé. Le cas échéant, une actualisation a toutefois été effectuée et la terminologie a été adaptée en fonction des nouvelles définitions utilisées. Seules les nouveautés sont développées et explicitées dans le présent exposé des motifs. Pour le reste, il est donc renvoyé aux travaux parlementaires de la loi du 27 avril 2016 relatif à des mesures complémentaires en matière de lutte contre le terrorisme (DOC 54 1727/001 et suivants) et aux rapports au Roi des arrêtés royaux d'exécution précités.

3. Méthode de travail

Un groupe de travail "restreint", composé de la Direction générale de la législation du SPF Justice et des acteurs de terrain que sont l'OCAM, la Police fédérale, le SGRS et la VSSE s'est réuni à plusieurs reprises pour préparer un premier projet de texte. Ensuite, d'autres acteurs essentiels ont participé à un second groupe de travail "élargi". Il s'agit du ministère public, du SPF Affaires

2. Doelstelling van het ontwerp

Het ontwerp strekt enerzijds toe om de bepalingen in de wet op het politieambt met betrekking tot de gemeenschappelijke gegevensbanken "Terrorist Fighters" en "Haatpropagandisten" om te zetten in een specifieke wet en anderzijds om de T.E.R.-strategie inzake de gemeenschappelijke gegevensbank en de Lokale Taskforces aan te scherpen. Die versterking gebeurt op verschillende manieren. Eerst en vooral gaat het erom deze wetgeving te vereenvoudigen en leesbaarder te maken. Daartoe werden een aantal bestaande bepalingen herwerkt, zowel in hun bewoording als in hun structuur. Vervolgens worden zoveel mogelijk elementen uit de koninklijke uitvoeringsbesluiten in de wet opgenomen om eraan een sterkere juridische grondslag te verschaffen, met name op het gebied van de bescherming van personen ten opzichte van de verwerking van persoonsgegevens op het vlak van de categorieën verwerkte gegevens. Doel is ook om in het kader van de Strategie T.E.R. de klemtoon te leggen op het noodzakelijke overleg tussen veiligheidsprofessionals over de gegevens in de gemeenschappelijke gegevensbank T.E.R., die het met elkaar eens moeten zijn over de wenselijkheid van het nemen van maatregelen wanneer een entiteit in de gemeenschappelijke gegevensbank wordt geregistreerd.

Er moet worden opgemerkt dat de meeste bestaande artikelen van de wet op het politieambt of de koninklijke besluiten "TF" en "HP" in dit ontwerp zijn overgebracht zonder inhoudelijke wijziging. Aangezien het ontwerp het bestaande dispositief *de facto* behoudt, blijft de verantwoording die aan de basis van de goedkeuring van deze bepalingen ligt, bijgevolg van toepassing en wordt ze in deze memorie niet opnieuw herhaald. In voorkomend geval werden er zaken geactualiseerd en werd de terminologie aangepast aan de nieuwe gehanteerde definities. Enkel de nieuwe zaken worden in deze memorie van toelichting uiteengezet en toegelicht. Voor het overige wordt dus verwezen naar de parlementaire werkzaamheden van de wet van 27 april 2016 inzake aanvullende maatregelen ter bestrijding van terrorisme (DOC 54 1727/001 en verdere) en naar de verslagen aan de Koning van de voornoemde koninklijke uitvoeringsbesluiten.

3. Werkwijze

Een "beperkte" werkgroep, bestaande uit het directoraat-generaal Wetgeving van de FOD Justitie en actoren in het veld (het OCAD, de federale politie, de ADIV en de VSSE) is meermaals samengekomen om een eerste ontwerp van tekst voor te bereiden. Vervolgens hebben andere essentiële actoren deelgenomen aan een tweede "ruimere" werkgroep. Het gaat om het openbaar ministerie,

étrangères, du SPF Intérieur et de la Commission permanente de la police locale.

Les Communautés, en particulier les Maisons de Justice, ont également été associées au processus d'élaboration du texte pour ce qui concerne leur compétence. Ainsi une conférence interministérielle des Maisons de Justice a été organisée le 17 mars 2023. Suite à cette conférence interministérielle, la ministre des Maisons de Justice et de l'Aide à la jeunesse de la Fédération Wallonie-Bruxelles et le ministre compétent pour la Maison de Justice et l'Aide à la Jeunesse au sein de la Communauté germanophone ont chacun émis un avis favorable sur le projet le 7 avril 2023. Il en est de même pour la ministre flamande de la Justice et du Contrôle, de l'Environnement, de l'Énergie et du Tourisme, qui a rendu son avis le 21 avril 2023.

Par ailleurs, des avis ont été sollicités auprès de différentes autorités compétentes en la matière:

— le Collège des Procureurs généraux a rendu un avis le 26 mai 2023 dans lequel il n'a formulé aucune remarque et s'est montré favorable au projet;

— le Conseil d'État a rendu son avis 73.442/2, le 7 juin 2023;

— l'Autorité de Protection des Données (A.P.D.) a rendu un avis n° 97/2023 daté du 16 juin 2023. Le Comité permanent de contrôle des services de police (Comité P) a également rendu un avis à la même date;

— l'Organe de contrôle de l'information policière (C.O.C.) a rendu son avis le 20 juin 2023;

— le Comité permanent de contrôle des services de renseignements et de sécurité (Comité R) a rendu l'avis n° 004/CPR/2023 le 13 juillet 2023;

À titre complémentaire, l'avis de l'ordre des médecins, pour ce qui concerne le traitement des données relatives à la santé ainsi que celui des délégués généraux aux droits de l'enfant, pour ce qui concerne le traitement des données relatives aux mineurs ont également été demandés. L'ordre des médecins n'a toutefois remis aucun avis.

Le cas échéant, les adaptations résultant des avis seront explicitées dans les commentaires par article du projet.

Enfin, en application de l'article 8, § 2, 1°, de la loi du 15 décembre 2013 portant des dispositions diverses concernant la simplification administrative, les avant-projets de réglementation qui touchent à la sécurité

de FOD Buitenlandse Zaken, de FOD Binnenlandse Zaken en de Vaste Commissie van de Lokale Politie.

De gemeenschappen, inzonderheid de justitiehuisen, werden eveneens betrokken bij de uitwerking van de tekst waar het hun bevoegdheid betrof. Zo werd er op 17 maart 2023 een Interministeriële Conferentie voor de Justitiehuisen georganiseerd. Ingevolge daarvan hebben de minister bevoegd voor de Justitiehuisen en Hulpverlening aan de Jeugd van de Federatie Wallonië-Brussel en de minister bevoegd voor het Justitiehuis en Hulpverlening aan de Jeugd van de Duitstalige Gemeenschap elk op 7 april 2023 een gunstig advies verstrekt over het ontwerp. Dat geldt ook voor de Vlaamse minister van Justitie en Handhaving, Omgeving, Energie en Toerisme, die haar advies op 21 april 2023 heeft verstrekt.

Er werd ook om advies verzocht bij verschillende ter zake bevoegde autoriteiten:

— het College van procureurs-generaal heeft op 26 mei 2023 een advies verstrekt, waarin het geen opmerkingen heeft en met het ontwerp instemt;

— de Raad van State heeft op 7 juni 2023 advies nr. 73.442/2 verstrekt;

— de Gegevensbeschermingsautoriteit (GBA) heeft op 16 juni 2023 advies nr. 97/2023 verstrekt. Het Vast Comité van Toezicht op de politiediensten (Comité P) heeft ook op diezelfde datum een advies verstrekt;

— het Controleorgaan op de politionele informatie (COC) heeft op 20 juni 2023 advies verstrekt;

— het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten (Comité I) heeft op 13 juli 2023 advies nr. 004/CPR/2023 verstrekt.

Aanvullend werd tevens verzocht om het advies van de Orde der artsen met betrekking tot de verwerking van gezondheidsgerelateerde gegevens, alsook om dat van de algemeen afgevaardigden voor de rechten van het kind met betrekking tot de verwerking van gegevens betreffende minderjarigen. De Orde der artsen heeft evenwel geen advies verstrekt.

In voorkomend geval worden de aanpassingen ingevolge de adviezen in de artikelsgewijze bespreking toegelicht.

Ten slotte, met toepassing van artikel 8, § 2, 1°, van de wet van 15 december 2013 houdende diverse bepalingen inzake administratieve vereenvoudiging, worden de voorontwerpen van regelgeving die de nationale

nationale et à l'ordre public sont exceptés d'analyse d'impact.

COMMENTAIRE DES ARTICLES

CHAPITRE 1^{ER}

Dispositions générales

Article 1^{er}

Cet article établit le principe constitutionnel de la compétence législative.

Art. 2

Cet article précise une série de notions qui reviennent régulièrement dans le projet afin d'en faciliter sa lecture. La plupart des définitions sont celles qui existaient dans l'article 1^{er} de l'arrêté royal "TF" et de l'arrêté royal "PH". Certaines ont toutefois été retravaillées en vue d'être plus claires et précises par rapport aux réalités du terrain. Enfin, de nouvelles définitions ont été introduites dans le projet.

Ainsi, la terminologie des dispositions de la loi sur la fonction de police transposées dans le présent projet a été adaptée en fonction des nouvelles définitions contenues dans l'article 2.

Parmi ces définitions, nous trouvons notamment les suivantes:

1) Services de base

Les quatre services de base sont l'Organe de coordination pour l'analyse de la menace (OCAM), la police intégrée et les services de renseignement et de sécurité (Sûreté de l'État (VSSE) et le Service Général du Renseignement et de Sécurité (SGRS)). Il s'agit des services de base visés à l'article 1^{er}, 7°, de l'arrêté royal "TF", l'article 1^{er}, 8°, de l'arrêté royal "PH" et l'article 44/11/3^{ter}, § 1^{er}, alinéa 1^{er}, a) à c), de la loi sur la fonction de police.

Il s'agit de services répressifs ou d'analyse qui travaillent directement en première ligne avec les entités et les finalités T.E.R. ou dont le travail d'analyse porte sur ces entités et, qui sont conséquemment susceptibles d'avoir le plus de données relatives à ces entités ou de détecter prioritairement une nouvelle entité T.E.R.

veiligheid en de openbare orde aanbelangen uitgezonderd van de impactanalyse.

TOELICHTING BIJ DE ARTIKELEN

HOOFDSTUK 1

Algemene bepalingen

Article 1

Dit artikel bepaalt de grondwettelijke grondslag voor de wetgevende bevoegdheid.

Art. 2

Dit artikel verduidelijkt een reeks begrippen die regelmatig terugkeren in het ontwerp teneinde de lezing ervan te vergemakkelijken. De meeste definities zijn die uit artikel 1 van het koninklijk besluit "TF" en van het koninklijk besluit "HP". Sommige werden echter herwerkt opdat ze duidelijker en nauwkeurig zouden zijn ten opzichte van de realiteit in het veld. Ten slotte zijn in het ontwerp nieuwe definities opgenomen.

De terminologie uit de bepalingen van de wet op het politieambt die in dit ontwerp zijn omgezet, werd aldus aangepast op basis van de nieuwe definities in artikel 2.

Met name de volgende definities zijn in dit artikel opgenomen:

1) Basisdiensten

De vier basisdiensten zijn het Coördinatieorgaan voor de dreigingsanalyse (OCAD), de geïntegreerde politie en de inlichtingen- en veiligheidsdiensten (Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichting en Veiligheid (ADIV)). Het gaat om de basisdiensten die worden bedoeld in artikel 1, 7°, van het koninklijk besluit "TF", artikel 1, 8°, van het koninklijk besluit "HP" en artikel 44/11/3^{ter}, § 1, eerste lid, a) tot en met c), van de wet op het politieambt.

Het gaat om politie- of analysediensten die bij hun werk rechtstreeks in eerste lijn met de T.E.R.-entiteiten en -doeleinden te maken hebben of waarvan het analyserend werk op die entiteiten betrekking heeft en die bijgevolg het grootste aandeel gegevens met betrekking tot die entiteiten ter beschikking kunnen hebben of als allereerste een nieuwe T.E.R.-entiteit kunnen opsporen.

Le terme “Organe” de la définition des articles précités a été précisé et modifié en “l’Organe de coordination pour l’analyse de la menace (OCAM)” et ce, afin d’éviter une confusion avec d’autres types d’organes visés dans le projet.

2) Services partenaires

Il s’agit de services fédéraux ou appartenant à des entités fédérées qui sont spécifiquement identifiés comme partenaires dans le cadre des finalités de la banque de données commune.

Dans son avis n° 97/2023 du 16 juin 2023, l’Autorité de protection des données mentionne les “47 services partenaires ayant accès à la BDC dont il est question dans le Rapport d’activité 2019 du Comité R” (§ 11). Or, il s’agit d’une erreur d’interprétation d’un document technique adressé par le gestionnaire au Comité R, document qui reprenait la désignation technique des différents services et organismes administratifs qui ont un accès à la banque de données commune. Pour des besoins techniques légitimes, certains services, tels que la police intégrée ou les Maisons de Justice, disposent de plusieurs désignations dans la banque de données commune pouvant laisser penser qu’il y a une démultiplication des partenaires qui ont un accès à celle-ci. Cependant, il est bien sûr évident que seuls les services désignés par la loi, c’est-à-dire les quatre services de base et les douze services partenaires, ont un accès effectif à la banque de données commune.

Dans le même ordre d’idée, dans son avis du 13 juillet 2023, le Comité R indique que le nombre de services partenaires et la quantité de données à caractère personnel augmentent, par rapport à la situation actuelle, sans explication (§ 2). Il faut rappeler ici que la plupart des utilisateurs de la banque de données commune T.E.R. sont repris du dispositif actuel et rassembler dans un seul instrument juridique, il ne s’agit donc pas d’une nouveauté. En ce qui concerne les nouveaux utilisateurs ou les nouveaux accès, des explications complémentaires ont été apportées dans l’exposé des motifs ci-après.

Les services partenaires évoqués ci-avant sont:

— soit un service de l’État qui exécute des missions de law enforcement en deuxième ligne qui touchent directement aux finalités et entités T.E.R. (comme par exemple, le Ministère public, la CTIF, la Direction Générale des Etablissements Pénitentiaires du Service public fédéral Justice);

De term “Orgaan” van de definitie uit de voornoemde artikelen werd verduidelijkt en gewijzigd in “Coördinatieorgaan voor de dreigingsanalyse (OCAD)”, zulks om verwarring te voorkomen met andere soorten organen die in dit ontwerp worden beoogd.

2) Partnerdiensten

Het gaat om federale diensten of diensten die aan gefedereerde entiteiten toebehoren die specifiek zijn geïdentificeerd als partners in het kader van de doeleinden van de gemeenschappelijke gegevensbank.

In advies nr. 97/2023 van 16 juni 2023 maakt de Gegevensbeschermingsautoriteit gewag van de “47 partnerdiensten met toegang tot de GGB waarnaar wordt verwezen in het activiteitenverslag 2019 van Comité I” (§ 11). Dat is echter een foutieve interpretatie van een technisch document van de beheerder aan Comité I waarin de technische aanwijzing is opgenomen van de verschillende administratieve diensten en organen die toegang hebben tot de gemeenschappelijke gegevensbank. Om legitieme technische redenen beschikken sommige diensten, zoals de geïntegreerde politie en de justitiehuisen, over verschillende aanwijzingen in de gemeenschappelijke gegevensbank, wat de indruk zou kunnen wekken dat er almaar meer partners toegang ertoe hebben. Het spreekt echter voor zich dat enkel de bij de wet aangewezen diensten, met andere woorden de vier basisdiensten en de twaalf partnerdiensten, effectief toegang hebben tot de gemeenschappelijke gegevensbank.

In diezelfde trant merkt Comité I in het advies van 13 juli 2023 op dat “het aantal partnerdiensten en de hoeveelheid persoonsgegevens in vergelijking met de huidige situatie zonder uitleg toenemen” (§ 2). Er zij hier op gewezen dat de meeste gebruikers van de gemeenschappelijke gegevensbank T.E.R. uit de huidige bepalingen zijn overgenomen en samengebracht in één juridisch instrument, wat dus betekent dat dat niets nieuws is. De nieuwe gebruikers of nieuwe toegangen worden nader verklaard in de hiernavolgende memorie van toelichting.

De hierboven vermelde partnerdiensten zijn:

— ofwel een dienst van de staat die rechtshandvingsopdrachten in tweede lijn uitvoert die rechtstreeks betrekking hebben op de T.E.R.-doeleinden en -entiteiten (zoals het openbaar ministerie, de CFI, het directoraat-generaal Penitentiaire Inrichtingen van de Federale Overheidsdienst Justitie);

— soit un service de l'État qui vu l'exercice de ses missions est susceptible de rentrer en contact avec une personne T.E.R., et qui s'il ne connaît pas sa qualité T.E.R. peut lui délivrer des "prérogatives" au nom de l'État, notamment sous forme de documents administratifs lui permettant de s'établir en Belgique, d'exercer une profession rémunérée, (comme par exemple, l'Office des étrangers, les Affaires consulaires, la DG sécurité et prévention, le service des cultes et de la laïcité du SPF Justice).

1 ° Concernant la pertinence pour l'Office des étrangers (OE) d'avoir accès à l'ensemble de l'information reprise dans la banque de données commune, on peut préciser ce qui suit:

Dans le cadre de ses missions légales, l'OE est compétent pour l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers.

Les domaines dans lesquels l'OE exerce ses compétences sont relativement étendus: visas, contrôle des étrangers aux frontières extérieures, contrôle et suivi du séjour des étrangers sur le territoire, migration légale (séjour de plus de trois mois/90 jours), court séjour (séjour de moins de trois mois/90 jours), protection internationale, protection temporaire, retour, etc.

Le cadre juridique dans lequel il exerce ses compétences est formé de normes nationales mais également de normes européennes et internationales, directement applicables.

L'OE est ainsi chargé de la mise en œuvre de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers mais aussi, de manière plus ponctuelle, des lois particulières. Les règles contenues dans ces lois mettent en œuvre la politique nationale en matière de migration, de retour et d'asile et assurent l'exécution des obligations européennes et internationales de la Belgique dans ces domaines. En ce qui concerne la politique des visas et le retour, il y a lieu aussi de tenir compte de la coopération renforcée menée dans le cadre juridique et institutionnel du Benelux.

En matière de franchissement des frontières et de court séjour, l'OE joue un rôle central dans le cadre de la mise en œuvre des règles de l'acquis de Schengen, y compris dans le cadre des procédures relatives aux visas de court séjour et de transit aéroportuaire. Dans le futur, il participera également directement aux procédures relatives aux autorisations de voyage (système européen ETIAS).

— ofwel een dienst van de staat die bij de uitvoering van zijn opdrachten in contact kan komen met een T.E.R.-persoon en die, indien hij niet op de hoogte is van diens hoedanigheid als T.E.R., hem in naam van de staat "prerogatieven" kan verlenen, inzonderheid in de vorm van administratieve documenten aan de hand waarvan die zich in België kan vestigen en een bezoldigd beroep kan uitoefenen (zoals de Dienst Vreemdelingenzaken, Consulaire Zaken, de AD Veiligheid en Preventie, de dienst Erediensten en Vrijzinnigheid van de FOD Justitie).

1° Wat de relevantie van de toegang van de Dienst Vreemdelingenzaken (DVZ) tot alle informatie in de gemeenschappelijke gegevensbank betreft, kan het volgende worden gepreciseerd:

In het kader van zijn wettelijke opdrachten is de DVZ bevoegd voor de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen.

De DVZ heeft vrij ruime bevoegdheidsgebieden: visa, controle van vreemdelingen bij de buitengrenzen, controle en opvolging van het verblijf van vreemdelingen op het grondgebied, legale migratie (verblijf van meer dan drie maanden/90 dagen), kort verblijf (verblijf van minder dan drie maanden/90 dagen), internationale bescherming, tijdelijke bescherming, terugkeer, enz.

Het juridisch kader waarbinnen hij zijn bevoegdheden uitoefent, is niet alleen opgemaakt uit nationale normen, maar ook uit Europese en internationale normen, die rechtstreeks van toepassing zijn.

Op die manier staat de DVZ niet alleen in voor de tenuitvoerlegging van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, maar ook specifiek van de bijzondere wetten. De regels in die wetten geven uitvoering aan het nationale migratie-, terugkeer- en asielbeleid en verzekeren dat België de Europese en internationale verplichtingen op die vlakken nakomt. Wat het visum- en terugkeerbeleid betreft, dient er ook rekening te worden gehouden met de versterkte samenwerking in het juridische en institutionele kader van de Benelux.

Op het gebied van grensoverschrijding en kort verblijf speelt de DVZ een centrale rol in de tenuitvoerlegging van de regels van het Schengenacquis, waaronder de procedures voor de visa kort verblijf en de luchthaven-transitvisa. In de toekomst zal hij tevens rechtstreeks betrokken zijn bij de procedures voor reisvergunningen (Europees ETIAS-systeem).

Les actes de l'acquis de Schengen en matière de franchissement des frontières et de court séjour prennent généralement la forme de règlements européens et sont donc directement applicables dans l'ordre juridique belge (Code des visas, Code frontières Schengen, règlement SIS, règlement VIS, règlement EES, règlement ETIAS, etc.). Ce domaine est également régi par des accords bilatéraux conclus par l'Union européenne et/ou par la Belgique (accords d'exemption de visa, accords de facilitation des visas, etc.).

La lutte contre les menaces de l'ordre public et la sécurité nationale fait partie des objectifs qui sous-tendent les règles de l'acquis de Schengen et qui participent au bon fonctionnement l'espace Schengen, comme espace de liberté, de justice et de sécurité.

L'OE exerce également des compétences importantes en matière de protection internationale, laquelle est largement régie par le droit européen et le droit international. Il est en particulier chargé de l'enregistrement des demandeurs, de la détermination de l'État membre responsable de l'examen des demandes de protection internationale (règlement européen "Dublin") et du suivi du séjour des demandeurs et des bénéficiaires de ces statuts. En ce qui concerne les bénéficiaires de la protection internationale, il peut également demander au CGRA d'abroger ou de retirer le statut de protection internationale et, le cas échéant, mettre fin au séjour de ceux dont le statut a été retiré ou abrogé.

L'expérience du conflit en Ukraine a démontré (et démontre encore) que l'OE joue un rôle essentiel en matière de protection temporaire, notamment en ce qui concerne l'enregistrement des personnes déplacées.

L'ensemble des règles applicables en matière de migration et d'asile donnent les moyens de protéger l'ordre public et la sécurité nationale. Ces règles sont l'expression d'un principe de droit international public bien établi, les États ont le droit de contrôler, sans préjudice des engagements découlant pour eux de traités, l'entrée, le séjour et l'éloignement des non-nationaux. Ce contrôle implique de veiller à la protection des intérêts essentiels que sont l'ordre public et la sécurité nationale. La protection de ces intérêts sont des éléments essentiels du contrôle exercé par l'OE, à tous les stades du processus migratoire. L'action de l'OE est donc nécessairement guidée par cet objectif.

Et c'est particulièrement le cas lorsqu'il est question de terrorisme et de radicalisme ou d'autres infractions graves liées à ces phénomènes.

De handelingen van het Schengenacquis inzake grensoverschrijding en kort verblijf nemen doorgaans de vorm aan van Europese verordeningen en zijn dus rechtstreeks van toepassing in de Belgische rechtsorde (Visumcode, Schengengrenscore, SIS-verordening, VIS-verordening, EES-verordening, ETIAS-verordening, enz.). Dergelijke zaken worden eveneens geregeld door bilaterale akkoorden gesloten door de Europese Unie en/of door België (visumvrijstellingsovereenkomsten, visumversoepelingsovereenkomsten enz.).

De bestrijding van de bedreiging van de openbare orde en de nationale veiligheid zijn een van de doelstellingen die het Schengenacquis onderschragen en die de goede werking van de Schengengebied als ruimte van vrijheid, veiligheid en recht bevorderen.

De DVZ oefent tevens belangrijke bevoegdheden uit op het gebied van internationale bescherming, dat in ruime mate wordt beheerst door het Europees en internationaal recht. Hij is inzonderheid belast met de registratie van de verzoekers, de bepaling van de lidstaat die verantwoordelijk is voor de behandeling van het verzoek om internationale bescherming ("Dublinverordening") en de opvolging van het verblijf van de verzoekers en van de personen met dergelijke statuten. Voor wat betreft de personen die internationale bescherming genieten, kan hij tevens het CGVS verzoeken het statuut van internationale bescherming in te trekken of op te heffen en, in voorkomend geval, het verblijf van die waarvan het statuut is ingetrokken of opgeheven, beëindigen.

Het conflict in Oekraïne heeft aangetoond (en doet dat nog steeds) dat de DVZ een sleutelrol speelt op het stuk van tijdelijke bescherming, met name voor wat de registratie van ontheemden betreft.

Alle toepasselijke regels inzake migratie en asiel samen leveren de middelen op om de openbare orde en de nationale veiligheid te beschermen. Die regels zijn de veruitwendiging van een goed verankerd beginsel van internationaal publiek recht: de Staten hebben het recht om, zonder afbreuk te doen aan de rechten die opgenomen zijn in verdragen, de binnenkomst, het verblijf en de verwijdering van vreemdelingen te controleren. Die controle impliceert het toezien op de bescherming van de essentiële belangen die de openbare orde en de nationale veiligheid uitmaken. De bescherming van die belangen zijn kernelementen van de controle die de DVZ uitoefent tijdens alle fasen van het migratieproces. Die doelstelling vormt dus noodzakelijkerwijs de leidraad voor de handelingen van de DVZ.

Dat is inzonderheid het geval wanneer er sprake is van terrorisme en radicalisme of andere ernstige misdrijven die met die verschijnselen verband houden.

Pour rappel, des mesures drastiques ont été prises durant ces dernières années pour que l'OE (et le CGRA) soit mieux armé face aux menaces terroristes ou liées au terrorisme, en réaction à la vague d'attentats qui ont été perpétrés un peu partout dans le monde, y compris en Belgique et dans d'autres pays voisins de l'Union européenne.

La loi du 15 décembre 1980 a aussi subi plusieurs modifications: les règles en matière de protection internationale ont été modifiées en 2016 afin que l'OE et le CGRA disposent des bases légales leur permettant de mieux prendre en considération la menace sécuritaire dans le cadre des procédures de protection internationale et d'adopter les mesures appropriées (refus, abrogation ou annulation du statut et, le cas échéant, retrait ou fin du séjour); et, les règles régissant la fin de séjour et l'éloignement des étrangers ont été modifiées en 2017 afin de renforcer la protection de l'ordre public et de la sécurité nationale.

Très récemment, le ministre a été investi du pouvoir de signaler aux fins de non-admission des étrangers qui se trouvent en-dehors du territoire pour des raisons d'ordre public ou de sécurité nationale. Un article 26/1 a été inséré à cette fin dans la loi du 15 décembre 1980. Il vise à assurer l'exécution de l'article 24, paragraphe 1, point a), et paragraphe 2, du règlement 2018/1861. Cette mesure participe justement à la lutte contre, entre autres, les "*foreign terrorist fighters*" (FTF – au sens de l'actuel article 6, § 1^{er}, 1^o, de l'AR du 21 juillet 2016), enregistrés dans la BDC.

La Banque de données commune (BDC) fait partie des mesures adoptées en réaction aux attentats. Il est un outil qui a été développé dans le cadre du Plan R. Créée en 2016, l'Office des étrangers, en tant que service d'appui, y a accès depuis le 20 mars 2017.

La BDC est un outil de partage d'informations non classifiées en temps réel. L'Office des étrangers a un droit de lecture et d'écriture dans la base de données. Cet accès n'est pas uniquement justifié par l'accès que peut avoir l'Office des étrangers aux informations pertinentes dans le cadre du suivi de ses dossiers asile et migration et des décisions qui peuvent en découler en application de la loi de 1980; mais l'Office encode également des données utiles et pertinentes, entre autres, pour le suivi assuré par les services de sécurité et de renseignement. La cellule radicalisme de l'Office est chargée à titre principal de l'alimentation de données actuelles concernant la situation administrative des personnes reprises dans

Ter herinnering: er zijn de afgelopen jaren drastische maatregelen genomen om de DVZ (en het CGVS) beter te wapenen tegen terroristische of terrorisme­gerelateerde dreiging, als reactie op een aanslagengolf die verspreid over de hele wereld is gepleegd, zo ook in België en in andere buurlanden in de Europese Unie.

De wet van 15 december 1980 heeft eveneens verschillende wijzigingen ondergaan: de regels op het stuk van internationale bescherming werden in 2016 gewijzigd zodat de DVZ en het CGVS wettelijke grondslagen hebben om beter rekening te houden met de veiligheidsdreiging in het kader van de procedures inzake internationale bescherming en om gepaste maatregelen te kunnen nemen (weigering, opheffing of annulatie van het statuut en, in voorkomend geval, intrekking of beëindiging van het verblijf), en ook de regels inzake de beëindiging van het verblijf en de verwijdering van vreemdelingen werden in 2017 gewijzigd om de bescherming van de openbare orde en de nationale veiligheid te versterken.

Onlangs heeft de minister de bevoegdheid gekregen om vreemdelingen buiten het grondgebied te signaleren met het oog op weigering van toegang om redenen van openbare orde en nationale veiligheid. Daartoe werd er een artikel 26/1 ingevoegd in de wet van 15 december 1980. Het strekt tot tenuitvoerlegging van artikel 24, lid 1, onder a), en lid 2, van Verordening 2018/1861. Die maatregel vormt net een schakel in de bestrijding van onder meer de "*foreign terrorist fighters*" (FTF's, in de zin van het huidige artikel 6, § 1, 1^o, van het koninklijk besluit van 21 juli 2016), die in de gemeenschappelijke gegevensbank worden opgenomen.

De gemeenschappelijke gegevensbank (GGB) is een van de maatregelen die is aangenomen als reactie op de aanslagen. Het is een tool die werd ontwikkeld in het kader van Plan R en waartoe de Dienst Vreemdelingen­zaken sinds 20 maart 2017 als steundienst toegang heeft.

De GGB is een tool om niet-geclassificeerde informatie realtime te delen. De Dienst Vreemdelingen­zaken heeft een lees- en schrijfrecht in de gegevensbank. Rechtvaardiging voor die toegang is niet alleen het feit dat de Dienst Vreemdelingen­zaken toegang kan hebben tot relevante informatie bij de opvolging van zijn asiel- en migratiedossiers en de mogelijke daaropvolgende beslissingen overeenkomstig de wet van 1980, maar ook het feit dat hij onder meer nuttige en relevante gegevens invoert voor de opvolging door de veiligheids- en inlichtingendiensten. De cel Radicalisme van de Dienst Vreemdelingen­zaken staat in hoofdzaak in voor de invoer van actuele gegevens die verband houden met

la banque de données et relevant de la compétence du ministre à l'asile et à la migration.

La BDC est un outil utile à l'accomplissement des missions légales de l'OE, en particulier pour évaluer la dangerosité des personnes soumises à son contrôle et assurer la légalité des décisions prises à leur égard.

Afin que l'Office puisse exercer ses missions légales et lorsqu'il prend une décision ayant un impact pour l'étranger basée sur des faits ayant trait à la sécurité nationale, la décision est basée sur des éléments émanant des services de sécurité et de renseignement en ce compris la banque de données commune.

Ces éléments sont repris dans la motivation formelle de l'acte administratif. Les documents sur lesquels l'Office se base (pour autant qu'ils ne soient pas classifiés) sont versés au dossier administratif de l'étranger.

Dans certains cas, l'Office doit se prononcer dans un délai particulièrement court et notifier sa décision dans les plus brefs délais. Par exemple, lorsqu'un étranger est intercepté à la frontière belge (refus d'entrée) ou sur le territoire (par exemple: décision de maintien en un lieu déterminé en vue d'un éloignement) et qu'une décision doit être prise au plus vite.

Enfin, différents articles de la loi de 1980 susmentionnée impliquent également que l'Office des étrangers doive pouvoir être informé des faits qui ont un impact en matière de sécurité nationale et conséquemment sur la situation administrative de l'étranger (art. 1, § 2, 3, 7, 8bis, § 1^{er}, 13, § 1^{er}, 15bis, § 1^{er}, 16bis, 19, § 1^{er}, 21, 22, § 1^{er}, 23, § 2, 24, 26, 26/1, 29, 30bis, § 4, 39/79, § 1^{er}, 43, § 1^{er}, 44bis, § 1^{er}, 44quinquies, § 1^{er}, 44septies, § 1^{er}, 44nonies, § 1^{er}, 45, § 1^{er}, 52/4 (ancien 52bis), 55/3/1, § 1^{er}, 55/4, § 2, 57/6/1, § 1^{er}, 57/7, § 3, 61/1/3, § 1^{er}, 61/1/4, § 2, 61/1/7, § 1^{er}, 61/1/13, 61/1/14, 61/2, § 3, 61/3, § 3, 61/4, § 1^{er}, 61/7, § 1, 61/8, § 2, 61/13/6, § 1^{er}, 61/13/7, 61/13/14, § 2, 62, § 2, 74/5, 74/6, § 1^{er}, 74/11, § 2, 74/14, § 1^{er}). Dans le cadre européen, on peut citer le Code des visas (article 32, § 1^{er}, a), points v et vi, lu en combinaison avec l'article 21; l'article 22 (consultation préalable) et l'article 31 (information postérieure); articles 33, 34, 35 et 36.), le Code frontières Schengen (article 14, en combinaison avec l'article 6, § 1^{er}, d) et e), le règlement SIS 2018/1860 (art. 4, § 1, o); art. 9, § 1, d); art. 10, d) et art. 11, d)), le règlement SIS 2018/1861 (art. 1^{er}; art. 3, 18); art. 21, § 2; art. 24, § 1^{er}, a) et § 2, b); art. 27, d); art. 28, d); art. 29, d); art. 34, § 1^{er}, a), b) et d) à e);

de l'administratieve situatie van de personen in de gegevensbank die onder de bevoegdheid van de minister bevoegd voor Asiel en Migratie vallen.

De GGB is een nuttige tool voor de uitoefening van de wettelijke opdrachten van de DVZ, inzonderheid om te evalueren in welke mate de personen die aan zijn controle onderworpen zijn, gevaarlijk zijn, alsook om te verzekeren dat de beslissingen jegens hen wettig zijn.

Opdat de Dienst Vreemdelingenzaken zijn wettelijke opdrachten kan uitoefenen en wanneer hij een beslissing neemt die een impact heeft voor de vreemdeling gebaseerd op feiten die verband houden met de nationale veiligheid, stoelt de beslissing op elementen afkomstig van de veiligheids- en inlichtingendiensten, met inbegrip van de gemeenschappelijke gegevensbank.

Die elementen worden opgenomen in de uitdrukkelijke motivering van de bestuurshandeling. De documenten waarop hij zich baseert (voor zover ze niet geclassificeerd zijn), worden onder het administratief dossier van de vreemdeling opgenomen.

In sommige gevallen moet de Dienst Vreemdelingenzaken zich in een bijzonder korte termijn uitspreken en zo snel mogelijk kennisgeven van zijn beslissing, bijvoorbeeld wanneer een vreemdeling wordt onderschept aan de Belgische grens (weigering tot binnenkomst) of op het grondgebied (bijvoorbeeld: beslissing tot vasthouding op een welbepaalde plaats met het oog op verwijdering) en er zo snel mogelijk een beslissing moet worden genomen.

Tot slot houden verschillende artikelen van de voormelde wet van 1980 in dat de Dienst Vreemdelingenzaken op de hoogte moet kunnen zijn van de feiten die een impact hebben op de nationale veiligheid en bijgevolg op de administratieve situatie van de vreemdeling (art. 1, § 2, 3, 7, 8bis, § 1, 13, § 1 15bis, § 1, 16bis, 19, § 1, 21, 22, § 1, 23, § 2, 24, 26, 26/1, 29, 30bis, § 4, 39/79, § 1, 43, § 1, 44bis, § 1, 44quinquies, § 1, 44septies, § 1, 44nonies, § 1, 45, § 1, 52/4 (oud 52bis), 55/3/1, § 1, 55/4, § 2, 57/6/1, § 1, 57/7, § 3, 61/1/3, § 1, 61/1/4, § 2, 61/1/7, § 1, 61/1/13, 61/1/14, 61/2, § 3, 61/3, § 3, 61/4, § 1, 61/7, § 1, 61/8, § 2, 61/13/6, § 1, 61/13/7, 61/13/14, § 2, 62, § 2, 74/5, 74/6, § 1, 74/11, § 2, 74/14, § 1). Op Europees vlak zijn er bijvoorbeeld de Visumcode (art. 32, lid 1, onder a), punten v en vi, in samenhang gelezen met art. 21, art. 22 (voorafgaande raadpleging), art. 31 (informatie achteraf), art. 33, 34, 35 en 36), de Schengengrenscore (art. 14, in samenhang met art. 6, lid 1, onder d) en e)), SIS-verordening nr. 2018/1860 (art. 4, lid 1, onder o), art. 9, lid 1, onder d), art. 10, onder d) en art. 11, onder d)), SIS-verordening nr. 2018/1861 (art. 1, art. 3, onder 18), art. 21, lid 2, art. 24, lid 1, onder a) en lid 2, onder b), art. 27, onder d), art. 28, onder d), art. 29,

art. 41, § 5), le règlement VIS et le règlement ETIAS (règlement 2018/1240).

2° Concernant l'Administration générale des douanes et accises et la nécessité d'avoir un accès à l'ensemble de l'information reprise dans la banque de données commune, cela se justifie pour les raisons suivantes:

De manière générale, il faut rappeler qu'elle a pour mission de protéger la société et de garantir la sécurité des citoyens. Pour ce faire, elle travaille au niveau national et international avec d'autres SPF et d'autres services répressifs, principalement dans la lutte contre la fraude, la criminalité organisée et le terrorisme. Par ailleurs, dans le cadre du nouveau plan de sécurité pour l'aéroport de Brussels Airport pour la période 2022-2025, adopté sur la base des recommandations de la commission d'enquête parlementaire suite aux attentats terroristes du 22 mars 2016, la coopération entre la Douane, la police, la justice et la province ainsi que les divers partenaires de sécurité sera intégrée dans une structure faïtière qui facilitera la lutte contre la criminalité et le terrorisme grâce à un flux d'informations plus fluide, une expertise partagée et une répartition claire des rôles. Le nouveau plan de sécurité met l'accent sur des phénomènes de sécurité prioritaires dont la radicalisation, l'extrémisme violent et le terrorisme.

Dans le contexte de la mission des autorités douanières, telle que définie à l'article 3 du règlement (UE) n° 952/2013 établissant le code des douanes de l'Union (*Union Customs Code – UCC*), la douane est principalement chargée de surveiller le commerce international de l'Union et de contribuer à la sécurité de la chaîne logistique. L'article 3 exige en outre que les autorités douanières prennent des mesures pour assurer la sécurité et sûreté de l'Union et de ses résidents, le cas échéant en coopération étroite avec d'autres autorités.

À la suite des attaques terroristes du début du 21^e siècle, les compétences des douanes en matière de sécurité ont encore été étendus. Au sein du département de la gestion des risques, l'analyse des risques en matière de sécurité et de sûreté est spécifiquement réalisée sur les marchandises entrant sur le territoire douanier de l'Union, conformément au code des douanes de l'Union et à ses règlements délégués et d'exécution (RD 2015/2446 et RE 2015/2447). Ce système actuel de contrôle des importations (*Import Control System – ICS*) évoluera vers un système de pré-dédouanement ACI (*cargo information system – ICS2*) en application de l'article 127, alinéa 6, du règlement 952/2013. Ce

onder d), art. 34, lid 1, onder a), b) en d) tot e), art. 41, lid 5), de VIS-verordening en de ETIAS-verordening (Verordening nr. 2018/1240).

2° Dat de Algemene Administratie van de Douane en Accijnzen toegang moet hebben tot alle informatie in de gemeenschappelijke gegevensbank, wordt gerechtvaardigd om de volgende redenen:

Op algemene wijze moet eraan worden herinnerd dat ze als opdracht heeft de samenleving te beschermen en de veiligheid van de burgers te verzekeren. Om die taken uit te voeren werkt ze nationaal en internationaal samen met andere federale overheidsdiensten en voornamelijk andere wetshandhavingdiensten in de strijd tegen fraude, georganiseerde misdaad en terrorisme. In het kader van het nieuwe veiligheidsplan voor Brussels Airport voor de periode 2022-2025, dat is aangenomen op basis van de aanbevelingen van de parlementaire onderzoekscommissie ten gevolge van de terroristische aanslagen van 22 maart 2016, is de samenwerking tussen douane, politie, justitie en provincie alsook de verschillende veiligheidspartners opgenomen in een overkoepelende structuur ter bevordering van de bestrijding van criminaliteit en terrorisme dankzij een vlottere informatiestroom, gedeelde deskundigheid en een duidelijke rollenverdeling. In het nieuwe veiligheidsplan wordt de nadruk gelegd op de prioritaire veiligheidsfenomenen, zoals radicalisering, gewelddadig extremisme en terrorisme.

In de context van de missie van de douaneautoriteiten, zoals vastgelegd in artikel 3 van Verordening (EU) nr. 952/2013 tot vaststelling van het douanewetboek van de Unie (*Union Customs Code – UCC*), is de douane primair verantwoordelijk voor het toezicht op de internationale handel van de Unie en draagt zij bij tot de veiligheid van de toeleveringsketen. Artikel 3 vereist verder dat de douaneautoriteiten maatregelen treffen om de veiligheid en beveiliging van de Unie en haar inwoners te waarborgen, in voorkomend geval in nauwe samenwerking met andere autoriteiten.

Naar aanleiding van de terroristische aanslagen begin 21^e eeuw werden de bevoegdheden van de douane inzake veiligheid verder uitgebreid. Binnen het departement Risicomanagement wordt specifiek een veiligheids- en beveiligingsrisicoanalyse uitgevoerd op goederen die het douanegebied van de Unie binnenkomen, dit overeenkomstig het douanewetboek van de Unie en zijn gedelegeerde en uitvoeringsverordeningen. (VO 2015/2446 en 2015/2447). Dit huidige Import Control System (ICS) zal in uitvoering van artikel 127, lid 6 van Verordening nr. 952/2013 evolueren naar een *Advanced Cargo Information System (ICS2)*. Dit systeem zorgt voor een pre-load beschikbaarheid

système garantit la disponibilité préalable des données de tous les modes de transport et l'échange d'informations relatives aux risques entre les autorités douanières au niveau de l'UE. Depuis la première version de ICS2, le 15 mars 2021 (article 106, alinéa 2 et 3, du règlement délégué 2015/2446), les douanes effectuent une analyse de risque de type *"bomb-in-the-box"* sur l'ensemble minimal de données visé à l'article 186, paragraphe 1, du Règlement d'exécution 2015/2447 aux fins de la détection des engins explosifs (EEI) envoyés par voie aérienne. Les informations nationales sur les individus liés au terrorisme constitueront la base de cette analyse de risque (article 186, alinéa 1, du règlement d'exécution 2015/2447).

Le département des enquêtes de l'Administration générale des douanes et accises est chargé de détecter et d'enquêter sur les fraudes à grande échelle et organisées dans divers domaines. Dans le cadre de ses attributions, elle a le pouvoir, entre autres, de fouiller des bâtiments, des véhicules et des marchandises, ainsi que d'utiliser certaines méthodes d'enquête spéciales, comme l'observation et l'opération d'informateurs.

Au sein de l'administration générale des douanes et accises, le département des enquêtes est également responsable de l'assistance mutuelle internationale et reçoit donc de nombreuses informations sur les personnes soupçonnées d'infractions douanières et d'accises ainsi que d'infractions de droit commun pour lesquelles les douanes sont compétentes (drogues, biens à double usage, armes, précurseurs d'explosifs, etc.).

Dans l'exercice de ses fonctions, l'administration chargée des enquêtes peut rencontrer des personnes radicalisées ou présentant des signes d'extrémisme ou de terrorisme, qui peuvent ou non figurer dans la banque de données commune T.E.R.

Les données des personnes soupçonnées d'être impliquées dans un crime ainsi que les données des personnes qui font l'objet d'une enquête sont conservées dans le système de base de données informatisée sur les crimes (CAMADA) de l'administration des enquêtes.

3° De même, la Direction générale Sécurité et Prévention du SPF Intérieur est compétente pour la délivrance des licences personnelles donnant accès au secteur délicat de la sécurité privée et particulière. Cela concerne tous les agents de sécurité privée en Belgique, quel que soit le lieu d'emploi (critique ou non). Cette licence est soumise à des conditions réglementaires, notamment l'examen des conditions de sécurité. Dans ce cadre, la DGSP a un intérêt certain de savoir si la personne demandeuse de ce badge est reprise

van gegevens van alle transportmodaliteiten en een uitwisseling van risico-gerelateerde informatie onder douaneautoriteiten op EU-niveau. Sinds Release I van ICS2, op 15 maart 2021 (artikel 106, lid 2 en 3, van Gedelegeerde Verordening 2015/2446), voert de douane een *"bomb-in-the-box"* risicoanalyse uit op de minimale dataset bedoeld in artikel 186, lid 1, van Uitvoeringsverordening 2015/2447 met als doel het opsporen van explosieven (IED's) die via de lucht verstuurd worden. Nationale informatie betreffende individuen gelinkt aan terrorisme zal de basis vormen van deze risicoanalyse (artikel 186, lid 1, van Uitvoeringsverordening 2015/2447).

De Administratie Opsporing van de Algemene Administratie van de Douane en Accijnzen heeft de opdracht grootschalige en georganiseerde fraude in diverse domeinen op te sporen en te onderzoeken. In het kader van haar opdracht heeft zij onder andere de bevoegdheid om gebouwen, voertuigen en goederen te doorzoeken, alsook om gebruik te maken van bepaalde bijzondere opsporingsmethoden, zoals observatie en informantenwerking.

De Administratie Opsporing is binnen de Algemene Administratie van de Douane en Accijnzen tevens verantwoordelijk voor de internationale wederzijdse bijstand en ontvangt aldus veel informatie over personen die verdacht worden van misdrijven inzake douane en accijnzen, alsook van misdrijven inzake gemeen recht waarvoor de douane bevoegd is (drugs, dual use-goederen, wapens, precursoren voor explosieven, enz.).

Bij de uitvoering van haar taken kan de Administratie Opsporing geconfronteerd worden met personen die geradicaliseerd zijn of tekenen van extremisme of terrorisme vertonen en al dan niet in de gemeenschappelijke gegevensbank T.E.R. voorkomen.

De gegevens van personen die ervan verdacht worden betrokken te zijn bij een misdrijf alsook de gegevens van personen die het voorwerp uitmaken van een onderzoek worden bijgehouden in het geautomatiseerd systeem "CAMADA" van de Administratie Opsporing.

3° Evenzo is de Algemene Directie Veiligheid en Preventie van de FOD Binnenlandse Zaken bevoegd voor de afgifte van de persoonsvergunningen die toegang verlenen tot de delicate sector van de private en bijzondere veiligheid. Dit betreft ondermeer alle bewakingsagenten in België ongeacht de plaats van tewerkstelling (kritisch of niet). Deze vergunning is afhankelijk van reglementaire voorwaarden waaronder het onderzoek naar de veiligheidsvoorwaarden. In dit kader heeft de ADVP er baat bij om te weten of de verzoekende persoon

comme *foreign terrorist fighter*, *homegrown terrorist fighter*, extrémiste potentiellement violent, personne condamnée pour terrorisme, propagandistes de haine ou comme entités à propos desquelles il existe de sérieux indices qu'elles puissent remplir les critères pour être considéré comme tel.

4° Il est également nécessaire que la Direction générale Affaires consulaires du SPF Affaires étrangères, dans le cadre de la délivrance d'un visa, puisse consulter la banque de données afin d'adapter sa décision. Par exemple, le visa pouvant être refusé.

En outre, dans un souci de centralisation et de lisibilité, cet article reprend désormais la liste des services énumérés à l'article 44/11/3^{ter}, § 2, alinéa 1^{er}, a) à i), de la loi sur la fonction de police mais également à l'article 7, § 1^{er}, alinéas 5 et 8 de l'arrêté royal "TF" et à l'article 7, § 1^{er}, alinéas 3, 6 et 8, de l'arrêté royal "PH". De nouveaux services partenaires sont donc ajoutés à la liste existante de la loi sur la fonction de police. Suite à l'avis du Conseil d'État 73.442/2 du 7 juin 2023, l'exposé des motifs a été complété concernant la nécessité de considérer le service des cultes et de la laïcité du Service public fédéral Justice et l'Administration générale de la Trésorerie du Service public fédéral Finances comme des services partenaires.

1° le service des cultes et de la laïcité du Service public fédéral Justice.

Le service des Cultes et de la Laïcité du SPF Justice est légalement compétent pour la reconnaissance des cultes et des organisations non confessionnelles. Il paie en outre les traitements des ministres des cultes et des délégués des communautés philosophiques non confessionnelles. Dans le cadre de ses compétences, il est nécessaire que ce service puisse interroger la banque de données commune T.E.R afin de vérifier que les ministres des cultes reconnus et délégués du Conseil central laïque rémunérés par l'État ne se retrouvent pas dans la banque de données commune T.E.R.

2° L'Administration générale de la Trésorerie du Service public fédéral Finances.

L'Administration générale de la Trésorerie est l'autorité compétente en matière de sanctions financières par le gel des fonds et des ressources économiques des personnes et entités qui commettent ou tentent de commettre des infractions terroristes, les facilitent ou y participent. La Trésorerie est gestionnaire des sanctions financières et acquiert donc à cet effet la connaissance

opgenomen is als *foreign terrorist fighter*, *homegrown terrorist fighter*, potentieel gewelddadige extremist, terrorismeveroordeeld, haatpropagandist of als entiteiten ten aanzien van wie er ernstige aanwijzingen bestaan dat zij de criteria om als zodanig te worden beschouwd.

4° Het is ook noodzakelijk dat het Directie-generaal Consulaire Zaken van de FOD Buitenlandse Zaken, in het kader van de afgifte van een visum, de gegevensbank zou kunnen raadplegen zijn beslissing aan te passen. Zo kan bijvoorbeeld kan het visum geweigerd worden.

Voorts omvat dit artikel ter wille van centralisering en leesbaarheid voortaan de lijst van de diensten die zijn opgesomd in artikel 44/11/3^{ter}, § 2, eerste lid, a) tot en met i), van de wet op het politieambt, maar eveneens in artikel 7, § 1, leden 5 en 8 van het koninklijk besluit "TF" en in artikel 7, § 1, leden 3, 6 en 8 van het koninklijk besluit "HP". Er worden dus nieuwe partnerdiensten toegevoegd aan de bestaande lijst van de wet op het politieambt. Ingevolge advies nr. 73.442/2 van 7 juni 2023 van de Raad van State werd de memorie van toelichting aangevuld met betrekking tot de noodzaak om de dienst Erediensten en Vrijzinnigheid van de Federale Overheidsdienst Justitie en de Algemene administratie van de Thesaurie van de Federale Overheidsdienst Financiën te beschouwen als partnerdiensten.

1° de dienst Erediensten en Vrijzinnigheid van de Federale Overheidsdienst Justitie.

De dienst Erediensten en Vrijzinnigheid van de FOD Justitie is bij wet bevoegd voor de erkenning van de erediensten en niet-confessionele organisaties. Daarnaast betaalt de dienst de wedden van de bedienaars van de erediensten en de afgevaardigden van niet-confessionele levensbeschouwelijke gemeenschappen. In het kader van deze bevoegdheden moet hij gegevens van de gemeenschappelijke gegevensbank T.E.R. kunnen opvragen teneinde na te gaan of de erkende bedienaars van de erediensten en de afgevaardigden van de Centrale Vrijzinnige Raad, die door de Staat worden uitbetaald, niet in de gemeenschappelijke gegevensbank T.E.R. staan.

2° de Algemene Administratie van de Thesaurie van de Federale Overheidsdienst Financiën.

De Algemene Administratie van de Thesaurie is de bevoegde overheid op het vlak van financiële sancties door het bevriezen van tegoeden en economische middelen van personen of entiteiten die terroristische misdrijven plegen of pogen te plegen, ze vergemakkelijken of eraan meewerken. Thesaurie is de beheerder van de financiële sancties en verwerft hierdoor dus kennis over

d'infractions et de données à caractère financier qui doivent être centralisées dans la banque de données commune pour assurer un échange de données intégré et optimal.

Dans la pratique, les avoirs de toutes les personnes qui ont rejoint un groupe terroriste en Syrie/Irak (FTF catégorie 1) ont été gelés. En outre, les avoirs d'un certain nombre d'autres entités ont déjà été gelés, notamment les avoirs de personnes condamnées pour des infractions terroristes. De plus, la Trésorerie est régulièrement contactée par des institutions financières lorsqu'elles entrent en contact avec des personnes dont les avoirs ont été gelés (ou pour lesquelles d'autres mesures financières ont été prises) par d'autres États (par exemple les États-Unis) dans un contexte de terrorisme, mais pas en Belgique. La Trésorerie doit procéder aux vérifications nécessaires et informer les institutions financières des conséquences éventuelles. L'un des éléments importants à cet égard est l'information consistant à savoir si la personne a été ou non reprise dans la banque de données commune T.E.R. La Trésorerie doit alors avoir la possibilité de vérifier quelles entités sont reprises en tant que telles dans la banque de données commune T.E.R.

Par ailleurs, l'Administration générale de la Trésorerie doit avoir la possibilité d'insérer elle-même les décisions qu'elle prend ainsi que de nombreuses informations pertinentes recueillies dans le cadre de sa compétence en matière de sanctions financières comme décrit dans l'arrêté royal du 28 décembre 2006 relatif aux mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le financement du terrorisme et la loi du 13 mai 2003 relative à la mise en œuvre des mesures restrictives adoptées par le Conseil de l'Union européenne à l'encontre d'États, de certaines personnes et entités. Sont visés ici: des montants financiers gelés, d'éventuels mouvements sur des comptes bancaires ou encore des assurances de tout type faisant l'objet d'une mesure de gel dans cette banque de données commune. Il est évident que ceci porte uniquement sur les informations relatives aux entités ayant déjà été reprises dans la Banque de données commune selon la procédure appropriée.

3° l'Administration générale des Maisons de Justice de la Communauté Française, le département Maison de Justice du Ministère de la Communauté Germanophone, l'Agence flamande pour la Justice et le Maintien, l'Administration générale de l'Aide à la Jeunesse de la Communauté Française, le département Aide à la Jeunesse de la Communauté Germanophone et l'Agence flamande Opgroeien.

misdrifven en financiële gegevens, die gecentraliseerd moeten worden in de gemeenschappelijke gegevensbank T.E.R. om een geïntegreerde en optimale informatie-uitwisseling te verzekeren.

In de praktijk werden de tegoeden van alle personen die zich aansloten bij een terroristische groepering in Syrië/Irak (F.T.F. categorie 1), bevroren. Daarnaast werden reeds tegoeden van een aantal andere entiteiten bevroren, en bijvoorbeeld van personen die veroordeeld werden voor terrorismemisdrijven. Bovendien wordt de Thesaurie regelmatig gecontacteerd door financiële instellingen wanneer deze in contact komen met personen waarvan andere landen (bijvoorbeeld de Verenigde Staten) de tegoeden bevroren (of waartegen andere financiële maatregelen getroffen werden) in de context van terrorisme, maar niet in België. De Thesaurie dient de nodige verificaties te doen en de financiële instellingen te informeren over de eventuele gevolgen hiervan. Een van de belangrijke elementen in deze, is de informatie of de persoon al dan niet opgenomen werd in de gemeenschappelijke gegevensbank T.E.R. De Thesaurie dient dus de mogelijkheid te hebben om te verifiëren welke entiteiten als dusdanig opgenomen zijn in de gemeenschappelijke gegevensbank T.E.R.

Daarnaast dient de Algemene administratie van de Thesaurie over de mogelijkheid te beschikken om zelf haar eigen beslissingen op te nemen in deze gemeenschappelijke gegevensbank, net als talrijke relevante informatie die zij verzamelt in het kader van haar bevoegdheden m.b.t. financiële sancties zoals beschreven in het koninklijk besluit van 28 december 2006 inzake specifieke beperkende maatregelen tegen bepaalde personen en entiteiten met het oog op de strijd tegen de financiering van het terrorisme en in de wet van 13 mei 2003 inzake de tenuitvoerlegging van de beperkende maatregelen die genomen worden door de Raad van de Europese Unie ten aanzien van Staten, sommige personen en entiteiten. Dit verwijst naar: de bedragen van de bevroren financiële middelen, eventuele bewegingen op bankrekeningen of verzekeringen allerlei die het voorwerp uitmaken van een maatregel tot bevroering. Het spreekt voor zich dat dit enkel betrekking heeft op de informatie betreffende de entiteiten die reeds werden opgenomen in de gemeenschappelijke gegevensbank volgens de gepaste procedure.

3° de Algemene Administratie van Justitiehuisen van de Franse Gemeenschap, het departement Justitiehuis van het Ministerie van de Duitstalige gemeenschap, het Vlaams Agentschap Justitie en Handhaving, de Algemene Administratie van de hulpverlening aan de jeugd van de Franse Gemeenschap, het departement Jeugdbijstand van de Duitstalige gemeenschap en het Vlaams Agentschap Opgroeien.

En ce qui concerne particulièrement le suivi réalisé par les Maisons de Justice et les autres agences et services visés à l'article 2, 3°, point I), dans le cadre de leurs missions légales d'accompagnement judiciaire et de la surveillance d'auteurs d'infractions, celui-ci est limité aux personnes pour lesquelles ces services partenaires ont reçu une mission sous la forme d'un mandat de suivi par une instance habilitée par ou en vertu d'une loi, d'un décret ou d'une ordonnance, ou sur la base d'un accord de coopération. Pour cibler ces personnes connues dans la banque de données commune T.E.R. et qui doivent être suivies par les maisons de justice et les agences et services précités, il est nécessaire de comparer les personnes qui sont dans la banque de données commune T.E.R. avec les personnes pour lesquelles elles ont reçu un mandat de suivi.

La Commission permanente de la police locale n'est plus reprise dans liste des services partenaires. En effet, étant donné sa raison d'être et les missions qui lui sont attribuées (essentiellement un Organe d'avis de la police et pas un Organe opérationnel), celle-ci n'a pas besoin d'un accès à la banque de données commune. Dans un souci de cohérence, ce service a donc été retiré de la liste.

En ce qui concerne le Centre de Crise national du Service public fédéral Intérieur, il faut préciser que dans les faits, ce sont les "unités opérationnelles" du Centre de Crise national, qui ont un besoin d'accès à la banque de données commune T.E.R. afin de savoir si la mesure administrative qu'elles prendraient à l'égard d'une entité, est pertinente eu égard à la confirmation qu'elles obtiendraient par cet accès.

Ainsi, l'Unité d'information des passagers (BelPIU, qui fait partie du "*National Travel Targeting Center*" au sein du Centre de crise National) est chargée d'analyser les données relatives aux voyageurs (Informations préalables sur les voyageurs / Dossiers passagers) à l'aide de listes de surveillance (par exemple, la Banque de données T.E.R.), de critères de risque et de recherches historiques dans le cadre de la lutte contre le terrorisme et la grande criminalité. L'une des listes de surveillance utilisées est la banque de données commune T.E.R. avec laquelle il est vérifié si les personnes figurant dans cette banque de données commune effectueront ou ont effectué un mouvement de voyage. Pour ce faire, le nom et le prénom tels qu'ils apparaissent dans la banque de données communes T.E.R. sont croisés avec les données des passagers collectées par les transporteurs. Conformément aux accords passés avec les services concernés, les résultats de cette analyse sont transmis à tous les acteurs concernés (police de l'aviation, unités de signalisation, OCAM, Sûreté, SGRS).

In het bijzonder is de opvolging door de Justitiehuizen en de andere in artikel 2, 3°, punt I), bedoelde agentschappen en diensten in het kader van hun wettelijke opdrachten van justitiële begeleiding van en toezicht op daders van misdrijven beperkt tot de personen ten aanzien van wie deze partnerdiensten een controleopdracht hebben gekregen vanwege een bij wet, decreet of ordonnantie, of op basis van een samenwerkingsakkoord gemachtigde instantie. Teneinde die personen te beogen die in de gemeenschappelijke gegevensbank T.E.R. zijn opgenomen en die door de justitiehuizen en de bovengenoemde agentschappen en diensten moeten worden opgevolgd, moeten de personen die in de gemeenschappelijke gegevensbank T.E.R. zijn opgenomen, worden vergeleken met de personen ten aanzien van wie zij een controleopdracht hebben gekregen.

Het vast comité van de lokale politie staat niet meer op de lijst van partnerdiensten. Gezien zijn bestaansreden en de hem toevertrouwde taken (in wezen een adviesorgaan van de politie, en niet een operationeel orgaan) heeft het namelijk geen toegang tot de gemeenschappelijke gegevensbank nodig. Omwille van de coherentie is deze dienst dus van de lijst geschrapt.

Wat het Nationaal Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken betreft, dient te worden verduidelijkt dat het in feite de "operationele eenheden" van het Nationaal Crisiscentrum zijn die toegang moeten hebben tot de gemeenschappelijke gegevensbank T.E.R., om te weten of de administratieve maatregel die ze zouden nemen ten aanzien van een entiteit pertinent is, gezien de bevestiging die ze zouden krijgen via die toegang.

De Belgische Passagiersinformatie Eenheid (BelPIU, een onderdeel van het "*National Travel Targeting Center*" binnen het Nationaal Crisiscentrum) heeft zo als opdracht passagiersgegevens (*Advance Passenger Information / Passenger Name Records*) te analyseren aan de hand van toezichtslijsten (bvb. gemeenschappelijke gegevensbank T.E.R.), risico-criteria en historische bevragingen in het kader van de strijd tegen terrorisme en ernstige criminaliteit. Eén van de gebruikte toezichtslijsten is de gemeenschappelijke gegevensbank T.E.R. waarbij nagegaan wordt of personen die voorkomen in deze gegevensbank een reisbeweging zullen maken of gemaakt hebben. Daarbij wordt de naam- en voornaam zoals deze in de gemeenschappelijke gegevensbank T.E.R. staat gekruist met passagiersgegevens die verzameld worden door vervoerders. Conform de gemaakte afspraken met de betrokken diensten, worden de hits die deze analyse opleveren overgemaakt aan alle relevante actoren (luchtvaartpolitie, seinende eenheden, OCAD, VSSE, ADIV).

La comparaison automatique effectuée, par exemple, par le système informatique de BelPIU entre la banque de donnée commune T.E.R., d'une part, et les données des passagers, d'autre part, doit faire l'objet d'une validation manuelle légalement requise avant que les données puissent être exportées de la base de données passagers. Afin de pouvoir vérifier lors de cette validation manuelle s'il s'agit réellement de la personne qui figure dans la base de données, le personnel de BelPIU doit pouvoir effectuer un certain nombre d'actions, notamment accéder au dossier de voyage, les recherches via open source (OSINT), les recherches via les bases de données mises à sa disposition (BNG, et autres bases de données de police).

Prenons l'exemple d'une personne x qui est connue dans la banque de donnée commune T.E.R. et voyage de Bruxelles à Oslo (et retour). Son dossier de réservation contient un prénom et un nom mais pas de date de naissance. Cependant, sur la base du nom et du prénom, il correspond à une entité dans la banque de données commune T.E.R. Étant donné qu'il y a nombre important de personnes en Belgique portant le même prénom et le même nom, le personnel de BelPIU doit vérifier s'il s'agit bien de la personne mentionnée dans la banque de données commune T.E.R. avant de transmettre les données de voyage à la police de l'aviation et/ou aux autres acteurs impliqués (il s'agit d'une mission requise par la loi, art. 24 § 4 de la loi du 25 décembre 2016). Sur la base de l'accès au dossier de voyage et de l'accès aux bases de données pertinentes (BNG, B.D.C., ...), le personnel de BelPIU peut conclure qu'il s'agit effectivement de la personne apparaissant dans la banque de données commune T.E.R. et pourra prendre les mesures de suivi nécessaires. Par exemple, la banque de données commune peut indiquer que la personne est déjà ou est encore à l'étranger ou a été arrêtée quelque part, ce qui permet à la personne de conclure qu'il ne s'agit pas de la personne concernée.

En outre, la banque de donnée commune T.E.R. peut alors toujours être complétée avec des informations dont dispose BelPIU: détails du vol de XX à YY, y compris le numéro de vol et l'arrivée/le départ prévu, les autres passagers connus, la date à laquelle le message a été envoyé à l'OCAM.

À noter qu'il a été tenu compte de la remarque du Comité R concernant le centre de crise (avis du 13 juillet 2023, § 37).

À noter également qu'en ce qui concerne la Direction Générale des Etablissements Pénitentiaires, la dénomination reprise dans la loi sur la fonction de police a été modifiée à l'article 2, 3^o, c), en ce sens que le terme "Direction générale des Etablissements pénitentiaires"

De automatische vergelijking die, bijvoorbeeld het computersysteem BelPIU maakt tussen de gemeenschappelijke gegevensbank T.E.R. enerzijds en de passagiersgegevens anderzijds moeten onderworpen worden aan een wettelijk verplichte manuele validatie alvorens gegevens geëxporteerd kunnen worden uit de gegevensbank passagiersgegevens. Om tijdens deze manuele validatie te kunnen nagaan of het werkelijk de persoon betreft die op in de gegevensbank voorkomt zal het personeel van BelPIU een aantal acties kunnen uitvoeren, m.n. inzage in het reisdoossier, opzoeken via open bronnen (OSINT), opzoeken via de voor hem voorhanden gegevensbanken (ANG, en andere politiebancen).

Nemen we het voorbeeld van een persoon x die is gekend in de gemeenschappelijke gegevensbank T.E.R. en reist van Brussel naar Oslo (en terug). Zijn reservatiedossier bevat een voor- en achternaam maar geen geboortedatum. Op basis van naam en voornaam zal hij echter wel matchen met de gemeenschappelijke gegevensbank T.E.R. Gezien er honderden personen zijn in België met dezelfde voor- en achternaam dient het personeel van BelPIU na te gaan of het werkelijk om het individu te gaan die in de gemeenschappelijke gegevensbank T.E.R. vermeld staat alvorens hij reisgegevens doorstuurt naar de luchtvaartpolitie en/of andere betrokken actoren (dit is een opdracht verplicht bij wet, art 24 § 4 wet van 25 december 2016). Op basis van inzage in het reisdoossier en inzage in relevante gegevensbanken (ANG, GGB, ...) concludeert het personeel van BelPIU dat het effectief gaat om de persoon die in de gemeenschappelijke gegevensbank T.E.R. voorkomt en de nodige vervolgacties te nemen. Zo kan de gemeenschappelijke gegevensbank T.E.R. bijvoorbeeld aangeven dat het individu zich al of nog in het buitenland bevindt of ergens is aangehouden op basis waarvan de persoon kan concluderen dat het hier niet gaat over de betreffende persoon.

Bovendien wordt de gemeenschappelijke gegevensbank T.E.R. telkens aangevuld met BelPIU informatie: vluchtgegevens van XX naar YY incl vluchtnummer en voorziene aankomst/vertrek, gekende medepassagiers, datum waarop bericht aan OCAM is overgemaakt.

Er moet worden opgemerkt dat er rekening is gehouden met de opmerking van Comité I met betrekking tot het crisiscentrum (advies van 13 juli 2023, § 37).

Opgemerkt dient ook te worden dat wat het Directoraat-generaal Penitentiaire Inrichtingen betreft, de benaming in de Politiewet gewijzigd is in artikel 2, 3^o c), in die zin dat de term "Directoraat-generaal Penitentiaire Inrichtingen" reeds zowel de centrale diensten van het DG EPI als

recouvre déjà tant les Services Centraux de la DG EPI que les services locaux c'est-à-dire les établissements pénitentiaires eux-mêmes. Par ailleurs, le droit de lecture à la banque de données commune T.E.R., le droit d'écriture de la DG EPI et le processus de validation interne relèvent des Services centraux de la DG EPI et non pas de chaque prison locale.

Tous ces services partenaires sont essentiels dans la lutte contre le terrorisme parce qu'ils traitent eux-mêmes de données contextuelles importantes et disposent dès lors des données et informations qui pouvaient enrichir celles des services de base. Ainsi c'est dans ce contexte que sur base de l'article 16, le Roi déterminera le type d'accès dans la banque de données commune T.E.R. dont disposera le service partenaire concerné ainsi que le contexte dans lequel il pourra utiliser ces droits.

Suite à l'avis du Comité R du 13 juillet 2023 (§ 36), l'Autorité nationale de sécurité est réintroduite dans le projet comme service partenaire et disposant d'un accès dans la banque de données commune T.E.R. dans le cadre de sa compétence en matière d'habilitations, attestations et avis de sécurité comme le prévoient l'article 7, § 1^{er}, alinéa 7, de l'arrêté royal "TF" et l'article 7, § 1^{er}, alinéa 2, de l'arrêté royal "PH".

Ainsi, cet organe doit pouvoir consulter la banque de données commune pour l'exercice de ses compétences et l'alimenter afin que les informations contenues dans celle-ci soient les plus complètes possibles.

En effet, il ressort du "rapport concernant le contrôle conjoint des banques de données communes *terrorist fighters* et prédicateurs de haine par le Comité permanent R et l'Organe de contrôle de l'information policière 2020" que l'ANS n'a, à ce jour, entrepris aucune démarche pour rendre effectif son accès à la banque de données commune. Le C.O.C. et le Comité permanent R estiment que cette "abstention, qui contrevient à la réglementation en application au moment du contrôle, fait courir des risques de sécurité non seulement en ce qui concerne le caractère systématique de la consultation des BDC mais aussi en ce qui concerne l'alimentation des BDC." (pp. 10-12).

Enfin, dans son avis du 13 juillet 2023, le Comité R estime qu'au vu du nombre important de services partenaires qui pourraient, en consultant la BDC T.E.R., prendre connaissance de crimes et délits non-encore poursuivis, il y a lieu de prévoir l'interaction entre le présent projet de loi et l'article 29 du livre premier du Code d'instruction criminelle (§ 40). Pour rappel, cet article

de plaatselijke diensten, d.w.z. de penitentiaire inrichtingen zelf, omvat. Bovendien vallen het leesrecht met betrekking tot de gemeenschappelijke gegevensbank T.E.R., het schrijfrecht van het DG EPI en het interne validatieproces onder de verantwoordelijkheid van de centrale diensten van het DG EPI en niet van de plaatselijke gevangenis.

Alle deze partnerdiensten spelen een sleutelrol in de bestrijding van terrorisme, omdat ze zelf belangrijke contextgegevens verwerken en dus over gegevens en informatie beschikken die een waardevolle toevoeging kunnen zijn voor die van de basisdiensten. In het kader daarvan bepaalt de Koning derhalve op grond van artikel 16 het type toegang tot de gemeenschappelijke gegevensbank T.E.R. waarover de partnerdienst in kwestie zal beschikken, alsook het kader waarin die laatste die rechten zal mogen aanwenden.

In navolging van het advies van Comité I van 13 juli 2023 (§ 36) is de Nationale Veiligheidsoverheid opnieuw in het ontwerp ingevoerd als partnerdienst die beschikt over toegang tot de gemeenschappelijke gegevensbank T.E.R. in het kader van zijn bevoegdheid inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, zoals bepaald in artikel 7, § 1, zevende lid, van het koninklijk besluit "TF" en artikel 7, § 1, tweede lid, van het koninklijk besluit "HP".

Zo moet dat orgaan de gemeenschappelijke gegevensbank kunnen raadplegen voor de uitoefening van zijn bevoegdheden en ze kunnen voeden, opdat de informatie erin zo volledig mogelijk zou zijn.

Uit het "Verslag betreffende de gezamenlijke controle van de gemeenschappelijke gegevensbanken *Terrorist Fighters* en Haatpropagandisten door het Vast Comité I en het Controleorgaan op de politionele informatie" uit 2020 blijkt namelijk dat de NVO thans nog geen enkele stap heeft ondernomen om haar toegang tot de gemeenschappelijke gegevensbank effectief te maken. Het COC en het Vast Comité I zijn het volgende van oordeel: "Haar gebrek aan handelen, in strijd met de toepasselijke regelgeving ten tijde van de controle, geeft aanleiding tot het ontstaan van veiligheidsrisico's, niet alleen wat betreft de stelselmatige raadpleging van de GGB maar ook wat betreft de levering van input voor de GGB." (blz. 10-12).

Tot slot is Comité I in het advies van 13 juli 2023 van oordeel dat, gelet op het grote aantal partnerdiensten dat door raadpleging van de GGB T.E.R. op de hoogte zou kunnen raken van nog niet vervolgte misdrijven, het aangewezen is te voorzien in een wisselwerking tussen dit ontwerp van wet en artikel 29 van boek I van het Wetboek van Strafvordering (§ 40). Ter herinnering:

concerne l'obligation de dénonciation des crimes et délits au procureur du Roi par tout fonctionnaire qui, dans l'exercice de ses fonctions, en a connaissance. L'encodage par un service d'une information constitutive d'un crime ou d'un délit dans la banque de données commune "T.E.R." ne dispense pas celui-ci d'en faire déclaration au ministère public sur la base de l'article 29 du Code d'instruction criminelle. Les finalités de la banque de données commune T.E.R. sont de l'ordre du partage et de la circulation d'information. Ce n'est en effet pas une outil dépôt de plainte ou une plateforme destinée à porter à la connaissance du Ministère public un fait nouveau.

3) Entité

La définition d'entité est issue de l'article 1^{er}, 10°, de l'arrêté royal "PH", à savoir "toute personne physique ou morale, association de fait, y compris l'ensemble des moyens utilisés". Dans l'ensemble du projet, on utilise le terme "entité" pour viser non seulement les personnes physiques et morales mais aussi les moyens de transport, ou les numéros de téléphones/comptes utilisés.

La définition d'entité vise deux statuts: celui d'entité validée et celui d'entité en pré-enquête.

L'"entité validée" vise toute personne physique majeure ou mineure de douze ans et plus, toute personne morale ou association de fait qui répond aux critères d'un *foreign terrorist fighter*, *homegrown terrorist fighter*, extrémiste potentiellement violent, personne condamnée pour terrorisme ou propagandiste de haine, ainsi que l'ensemble des moyens utilisés par celles-ci.

L'"entité en pré-enquête" vise toute personne physique majeure ou mineure de douze ans et plus, toute personne morale ou association de fait à propos de laquelle il existe des indices sérieux qu'elle puisse remplir les critères d'un *foreign terrorist fighter*, *homegrown terrorist fighter*, extrémiste potentiellement violent ou propagandiste de haine, ainsi que l'ensemble des moyens utilisés par celles-ci (cf. détails *infra*).

Conformément à l'avis du Conseil d'État 73.442/2 du 7 juin 2023, à l'avis n° 97/2023 de l'Autorité de protection des données du 16 juin 2023 (§§ 20-21) et à l'avis du Comité R du 13 juillet 2023 (§ 19), les catégories d'"entités" constituent un élément central, et donc essentiel, du dispositif en projet, qui doit en conséquence être fixé par le législateur. L'énumération de ces catégories est

dat artikel betreft de verplichting tot aangifte van misdaden en wanbedrijven aan de procureur des Konings door elke ambtenaar die in de uitoefening van zijn ambt daarvan kennis krijgt. De invoering door een dienst van informatie die een misdaad of wanbedrijf uitmaakt in de gemeenschappelijke gegevensbank "T.E.R.", ontslaat deze dienst niet van de aangifte ervan aan het Openbaar Ministerie op basis van artikel 29 van het Wetboek van Strafvordering. De doeleinden van de gemeenschappelijke gegevensbank T.E.R. houden verband met het delen en de doorstroming van informatie. Het is namelijk geen tool om klacht neer te leggen of een platform om een nieuw feit ter kennis van het openbaar ministerie te brengen.

3) Entiteit

De definitie van een entiteit komt uit artikel 1, 10°, van het koninklijk besluit "HP", namelijk "de natuurlijke personen, rechtspersonen, feitelijke verenigingen met inbegrip van alle aangewende middelen". De term "entiteit" doelt in het gehele ontwerp niet alleen op natuurlijke en rechtspersonen, maar ook op vervoersmiddelen of gebruikte telefoon-/rekeningnummers.

De definitie van entiteit betreft twee statussen: die van een gevalideerde entiteit en die van een entiteit in vooronderzoek.

De "gevalideerde entiteit" verwijst naar elke meerderjarige natuurlijke persoon of minderjarige natuurlijke persoon van twaalf jaar en ouder, elke rechtspersoon of feitelijke vereniging die beantwoordt aan de criteria van een *foreign terrorist fighter*, *homegrown terrorist fighter*, potentieel gewelddadige extremist, terrorismeveroordeelde of haatpropagandist, alsook alle de door hen aangewende middelen;

De "entiteit in vooronderzoek" verwijst naar elke meerderjarige natuurlijke persoon of minderjarige natuurlijke persoon van twaalf jaar en ouder, elke rechtspersoon of feitelijke vereniging ten aanzien waarvan er ernstige aanwijzingen bestaan dat ze kan voldoen aan de criteria van een *foreign terrorist fighter*, *homegrown terrorist fighter*, potentieel gewelddadige extremist of haatpropagandist, alsook alle de door hen aangewende middelen (zie details hieronder).

Overeenkomstig advies nr. 73.442/2 van 7 juni 2023 van de Raad van State, advies nr. 97/2023 van 16 juni 2023 van de Gegevensbeschermingsautoriteit (§§ 20-21) en het advies van Comité I van 13 juli 2023 (§ 19) vormen de categorieën van "entiteiten" een kernaspect en dus een essentieel element van het ontworpen dispositief, dat bijgevolg door de wetgever dient te worden vastgesteld.

donc ajoutée dans le présent projet, à l'article 2, 4°. Elles sont définies à l'article 2, 5° à 11°.

Il s'agit des catégories suivantes:

1° les *Foreign terrorist fighters* (F.T.F.) qui sont des résidents établis en Belgique ou qui y ont résidé, ayant ou non la nationalité belge et qui soit:

— se sont rendus dans une zone de conflit djihadiste dans le but de se rallier à des groupements organisant ou soutenant des activités terroristes ou de leur fournir un soutien actif ou passif (catégorie 1);

— ont quitté la Belgique pour se rendre dans une zone de conflit djihadiste dans le but de se rallier à des groupements organisant ou soutenant des activités terroristes ou de leur fournir un soutien actif ou passif (catégorie 2);

— sont en route vers la Belgique ou sont revenus en Belgique après s'être rendus dans une zone de conflit djihadiste où ils se sont ralliés à des groupements organisant ou soutenant des activités terroristes ou leur ont fourni un soutien actif ou passif (catégorie 3);

— ont volontairement ou non été empêchés de se rendre dans une zone de conflit djihadiste dans le but de se rallier à des groupements organisant ou soutenant des activités terroristes ou de leur fournir un soutien actif ou passif (catégorie 4);

— ont sérieusement l'intention de se rendre dans une zone de conflit djihadiste dans le but de se rallier à des groupements organisant ou soutenant des activités terroristes ou de leur fournir un soutien actif ou passif (catégorie 5);

Par zone de conflit djihadiste, il y a lieu d'entendre un territoire sur lequel se livre une lutte visant à propager, imposer ou protéger, de manière violente, une vision de l'Islam. Sur base de l'analyse stratégique de l'OCAM, les ministres de l'Intérieur et de la Justice proposent ce territoire comme "zone de conflit djihadiste" au Conseil national de sécurité. Les visions opérationnelles et politiques sont ainsi coordonnées en raison des mesures à prendre à l'égard de certaines personnes se rendant ou s'étant rendues dans une telle zone de conflit.

Dans son avis du 13 juillet 2023, le Comité R "n'aperçoit pas "dans les travaux préparatoires de justification quant au ciblage des personnes se rendant dans une zone de conflit jihadiste dans le but de se rallier à des

De opsomming van die categorieën is toegevoegd aan artikel 2, 4° van dit ontwerp. Ze worden gedefinieerd in artikel 2, 5° tot 11°.

Het betreft de volgende categorieën:

1° de *foreign terrorist fighters* (F.T.F.) die in België gevestigde bewoners zijn of die er verbleven hebben, die al dan niet de Belgische nationaliteit bezitten en die hetzij:

— naar een jihadistische conflictzone zijn afgereisd om er zich aan te sluiten bij of actieve of passieve steun te verlenen aan groeperingen die terroristische activiteiten uitvoeren of ondersteunen (categorie 1);

— vanuit België op weg zijn naar een jihadistische conflictzone om zich aan te sluiten bij, of actieve of passieve steun te verlenen aan groeperingen die terroristische activiteiten uitvoeren of ondersteunen (categorie 2);

— naar België onderweg of teruggekeerd zijn uit een jihadistische conflictzone waar zij zich aansloten bij, of actieve of passieve steun verleenden aan groeperingen die terroristische activiteiten uitvoeren of ondersteunen (categorie 3);

— gewild of ongewild verhinderd werden om naar een jihadistische conflictzone af te reizen om zich aan te sluiten bij, of actieve of passieve steun te verlenen aan groeperingen die terroristische activiteiten uitvoeren of ondersteunen (categorie 4);

— de ernstige intentie hebben te zullen vertrekken naar een jihadistische conflictzone om zich aan te sluiten bij, of actieve of passieve steun te verlenen aan groeperingen die terroristische activiteiten uitvoeren of ondersteunen (categorie 5).

Onder jihadistische conflictzone dient een grondgebied waarop strijd wordt geleverd om een stellingname binnen het islamitische geloof op een gewelddadige manier te propageren, op te leggen of te beschermen, te worden verstaan. De ministers van Binnenlandse Zaken en van Justitie, stellen, op basis van de strategische analyse van het OCAD, het grondgebied voor bij de Nationale Veiligheidsraad als "jihadistische conflictzone". Op die manier worden de operationele en politieke visies gecoördineerd omwille van de te nemen maatregelen ten aanzien van bepaalde personen die zich naar een dergelijke conflictzone begeven of begeven hebben.

In het advies van 13 juli 2023 ziet het Vast Comité I "in de voorbereidende werkzaamheden geen rechtvaardiging voor het viseren van personen die naar een jihadistisch conflictgebied reizen met het doel zich aan te sluiten bij

groupements terroristes ou de leur fournir un soutien actif ou passif, par rapport aux personnes se rendant dans le même but dans une zone de conflit “non-djihadiste”. Le Comité permanent R relève que le terrorisme n’est pas un phénomène exclusivement lié au djihadisme et recommande donc de justifier cette différence de traitement ou de la supprimer.” (§ 21). À cet égard, précisons que les FTF sont la seule catégorie d’entité qui est liée aux zones de conflit djihadiste, ce n’est pas le cas des autres catégories explicitées ci-après.

2° Les *Homegrown Terrorist Fighters* (H.T.F.) visent les personnes qui ne se sont pas rendues dans des zones de conflit mais pour lesquelles il existe des indications sérieuses qu’elles ont l’intention de commettre un attentat ou qu’elles donnent intentionnellement un soutien dans ce but.

Le *Homegrown Terrorist Fighter* est défini comme toute personne physique, ayant un lien avec la Belgique dès lors qu’au moins un des deux critères suivants est rempli:

a) il existe des indications sérieuses que cette personne a l’intention de recourir à la violence à l’encontre de personnes ou d’intérêts matériels, pour des motifs idéologiques ou politiques, dans le but d’atteindre leurs objectifs par la terreur, l’intimidation ou les menaces;

b) il existe des indications sérieuses que la personne donne intentionnellement un soutien, notamment logistique, ou financier, ou aux fins de formation ou recrutement, aux personnes visées au a) ou aux personnes enregistrées en tant que F.T.F. et pour lesquelles il existe des indications sérieuses qu’elles ont l’intention de commettre un acte violent.

Cette disposition se base sur la définition du terrorisme prévue à l’article 8, § 1^{er}, b) de la loi organique des services de renseignement et de sécurité du 30 novembre 1998, où il est également question des concepts d’ “intérêts matériels” et de “motifs idéologiques et politiques”. Une référence à cette définition est aussi reprise à l’article 3 de la loi du 10 juillet 2006 relative à l’analyse de la menace. Une terminologie identique figure maintenant dans la présente loi.

En ce qui concerne le premier des critères primaires susmentionnés, les “indications sérieuses” ne peuvent se fonder uniquement sur les motivations personnelles du potentiel H.T.F., mais également et surtout sur des actes matériels préparatoires d’un attentat.

terroristische groeperingen of deze actief of passief te steunen, in tegenstelling tot personen die met hetzelfde doel naar een “niet-jihadistisch” conflictgebied reizen. Het Vast Comité I merkt op dat terrorisme geen fenomeen is dat uitsluitend verband houdt met jihadisme en beveelt dan ook aan dit verschil in behandeling te rechtvaardigen of weg te werken.” (§ 21). In dat verband dient te worden verduidelijkt dat de FTF de enige categorie van entiteiten vormen die verband houdt met jihadistische conflictgebieden, wat voor de andere categorieën die hierna worden toegelicht niet het geval is.

2° *Homegrown Terrorist Fighters* (H.T.F.) richten zich op personen die niet zijn afgereisd naar conflictgebieden, maar waarvoor er ernstige vermoedens bestaan dat zij de intentie hebben om een aanslag te plegen of dat zij hieraan doelbewust steun leveren.

De *Homegrown Terrorist Fighter* wordt gedefinieerd als elke fysieke persoon waarbij er een aanknopingspunt is met België en vanaf het ogenblik dat er aan minstens één van beide volgende criteria is voldaan:

a) er bestaan ernstige aanwijzingen dat zij de intentie hebben om geweld te gebruiken tegen personen of materiële belangen om ideologische of politieke redenen met het doel hun doelstellingen door middel van terreur, intimidatie of dreigingen te bereiken;

b) er bestaan ernstige aanwijzingen dat de persoon doelbewust steun levert, meer bepaald logistiek, financieel of met opleidings- of rekruteringsdoeleinden, aan de personen geïdende in a) of aan personen die geregistreerd staan als F.T.F. en waarvoor er ernstige aanwijzingen bestaan dat zij de intentie hebben om een gewelddadige actie uit te voeren.

Deze bepaling werd gebaseerd op de definitie van terrorisme bepaald in artikel 8, § 1, b), van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, die eveneens de begrippen “materiële belangen” en “ideologische of politieke redenen” hanteert. Een verwijzing naar deze definitie werd ook opgenomen in artikel 3 van de wet van 10 juli 2006 betreffende de analyse van de dreiging. Dezelfde terminologie wordt nu hernomen in deze wet.

Wat het eerste criterium van de bovenvermelde primaire criteria betreft, mogen de “ernstige aanwijzingen” niet enkel gebaseerd zijn op de persoonlijke beweegredenen van de potentiële H.T.F., maar tevens en vooral op diens materiële handelingen ter voorbereiding van een aanslag.

Une indication sérieuse a trait à une situation qui peut être étayée par des éléments concrets. L'OCAM décide *in fine* quant à la validation comme H.T.F.

Les exemples suivants permettent de l'illustrer ce premier critère. Sera repris par exemple comme H.T.F. un partisan de l'État islamique qui, depuis une prison en Belgique, projette de commettre un attentat après sa libération, et ce pour le compte de l'État islamique. De même, un partisan belge de l'État islamique qui est sollicité ou inspiré depuis la Syrie ou l'Irak par des membres de l'État islamique en vue de commettre des attentats en Belgique sera également repris. Un militant d'extrême-droite préparant des actions terroristes contre un centre de réfugiés pour des motifs idéologiques pourra aussi être repris comme H.T.F. dans la banque de données commune T.E.R. Par contre, ne sera pas reprise comme H.T.F. une personne qui, par exemple, part se battre en Ukraine de l'Est.

En ce qui concerne le second critère, les exemples suivants permettent de l'illustrer. Sera repris par exemple comme H.T.F. une personne apportant volontairement un soutien financier à un groupe belge d'extrême-droite connu pour planifier des actes de terrorisme en Belgique ou encore une personne qui apporterait un soutien financier à une autre personne, cette dernière recrutant personnellement d'autres personnes en Belgique afin de les envoyer combattre dans une zone de conflit djihadiste. Par contre, ne sera pas reprise comme H.T.F. une personne belge radicalisée, sympathisante de l'État islamique, dès lors qu'elle n'apporte aucun soutien quelconque (logistique, financier, ...) à l'État islamique.

En ce qui concerne le lien avec la Belgique, il est précisé ici que ce qui importe, c'est de déterminer un lien fondé, qu'il soit d'ordre juridique et/ou factuel entre le H.T.F. et la Belgique. Par exemple, dans le cas d'un H.T.F., de nationalité belge qui aurait l'intention de réaliser un attentat en France, le lien retenu serait d'ordre juridique, la nationalité belge de l'intéressé. Dans le cas d'un H.T.F. de nationalité étrangère et résidant en France qui donnerait intentionnellement un soutien logistique à un groupe terroriste basé en Allemagne en vue de réaliser un attentat en Belgique, le lien retenu serait d'ordre factuel, c'est-à-dire le lieu de l'attentat potentiel, la Belgique. Il y a nécessité de maintenir une certaine flexibilité dans l'établissement du lien avec la Belgique. Cette relative flexibilité est encadrée par un double contrôle en termes de validation. Tout d'abord, dans le cadre de la validation des services impliqués dans la banque de données commune T.E.R., lorsqu'ils y introduisent des entités H.T.F., et ensuite, lors du

Een ernstige aanwijzing betreft een situatie die met concrete elementen kan worden ondersteund. Het OCAD beslist *in fine* over de validering als H.T.F.

Volgende voorbeelden laten toe om het eerste criterium te illustreren. Zo zal bijvoorbeeld een aanhanger van Islamitische Staat die vanuit een gevangenis in België een aanslag beraamt om na zijn vrijlating te plegen en dit voor rekening van Islamitische Staat, opgenomen worden als H.T.F. In diezelfde lijn zal een Belgische aanhanger van Islamitische Staat die vanuit Syrië of Irak door leden van Islamitische Staat wordt verzocht of geïnspireerd om aanslagen te plegen in België, worden opgenomen. Ook een militant van extreemrechts die terroristische acties plant tegen een opvangcentrum voor vluchtelingen omwille van ideologische motieven zal als H.T.F. kunnen worden opgenomen in de gemeenschappelijke gegevensbank T.E.R. Daarentegen zal een persoon die bijvoorbeeld vertrekt om in Oost-Oekraïne te gaan strijden, niet worden opgenomen als H.T.F.

Het tweede criterium kan worden geduid aan de hand van volgende voorbeelden. Zo zal bijvoorbeeld een persoon die vrijwillig financiële steun levert aan een Belgische extreemrechtse groep die gekend is voor het plannen van daden van terrorisme in België, opgenomen worden als H.T.F. Ook een persoon die financiële steun levert aan een andere persoon kan opgenomen worden als H.T.F., als deze laatste zelf andere personen in België rekruteert om te gaan strijden in een jihadistische conflictzone. Daarentegen zal een Belgische geradicaliseerde persoon die sympathiseert met Islamitische Staat niet worden opgenomen als H.T.F. indien hij geen enkele vorm van steun (logistiek, financieel, ...) levert aan Islamitische Staat.

Wat het aanknopingspunt betreft, met België, dient hier te worden gepreciseerd dat het belangrijk is een onderbouwd aanknopingspunt te bepalen tussen de H.T.F. en België, of dit nu juridisch en/of feitelijk van aard is. Bijvoorbeeld, in het geval van een H.T.F. met de Belgische nationaliteit, die de intentie zou hebben om een aanslag te plegen in Frankrijk, zou de weerhouden link van juridische aard zijn: de Belgische nationaliteit van de betrokkene. In het geval van een H.T.F. met een buitenlandse nationaliteit, die in Frankrijk verblijft, en die doelbewust logistieke steun zou verlenen aan een terroristische groep in Duitsland met de bedoeling om een aanslag te plegen in België, zou de weerhouden link van feitelijke aard zijn, het is te zeggen, de plaats van de mogelijke aanslag, België. Het is noodzakelijk om een zekere flexibilitéit te behouden in het vaststellen van een "aanknopingspunt" met België. Deze relatieve flexibilitéit wordt omkaderd door een dubbele controle op het vlak van validering. Een eerste controle gebeurt

processus de validation de la personne comme H.T.F. dans la banque de données commune T.E.R. par l'OCAM.

3° L'Extrémiste Potentiellement Violent (E.P.V.) est défini comme toute personne physique ayant un lien avec la Belgique et qui répond aux critères cumulatifs suivants:

a) elle a des conceptions extrémistes qui justifient l'usage de la violence ou de la contrainte comme méthode d'action en Belgique;

b) il existe des indications fiables qu'elle a l'intention de recourir à la violence, et ce en relation avec les conceptions extrémistes mentionnées en a).

En outre, l'E.P.V. doit répondre au minimum à l'une des trois conditions suivantes qui sont considérées comme étant des facteurs de risque quant à l'utilisation de la violence:

i) il entretient systématiquement des contacts sociaux au sein de milieux extrémistes;

ii) il a des problèmes psychiques constatés par un professionnel compétent en la matière;

iii) il a commis des actes ou il présente des antécédents qui peuvent être considérés comme:

— soit a) un crime ou un délit portant atteinte à ou menaçant l'intégrité physique ou psychique de tiers;

— soit b) des instructions ou des formations relatives à la fabrication ou l'utilisation d'explosifs, d'armes à feu ou d'autres armes ou substances nocives ou dangereuses, ou pour d'autres méthodes et techniques spécifiques en vue de commettre des infractions terroristes conformément à l'article 137 du Code pénal;

— soit c) des agissements en connaissance de cause constituant un soutien matériel en faveur d'une organisation ou d'un réseau terroriste/extrémiste;

— soit d) des agissements dont la nature indique un niveau de vigilance préoccupant de l'individu à l'égard de la sécurité.

L'E.P.V. est une personne physique ayant un lien avec la Belgique. Il peut s'agir d'un lien d'ordre juridique ou factuel. Le fait d'avoir la nationalité belge ou de disposer d'un droit de séjour en Belgique sont des exemples d'un lien d'ordre juridique. La personne concernée peut

door de partnerdiensten wanneer zij een potentiële H.T.F. ingeven in de gemeenschappelijke gegevensbank T.E.R. Een tweede controle gebeurt door het OCAD bij de validering van een persoon als H.T.F. in de gemeenschappelijke gegevensbank T.E.R.

3° De Potentieel Gewelddadige Extremist (P.G.E.) wordt gedefinieerd als elke natuurlijke persoon die een aanknopingspunt heeft met België en die voldoet aan de volgende cumulatieve criteria:

a) hij heeft extremistische opvattingen die het gebruik van geweld of dwang als actiemethode in België legitimeren;

b) er zijn betrouwbare aanwijzingen dat hij de intentie heeft om geweld te gebruiken, en dit in verband met de extremistische opvattingen vermeld in a).

Daarnaast dient de P.G.E. te voldoen aan minstens één van de drie volgende criteria die beschouwd worden als risicofactoren voor het gebruik van geweld:

i) hij heeft systematisch sociale contacten binnen extremistische milieus;

ii) er is een psychische problematiek vastgesteld door een daartoe gekwalificeerde deskundige;

iii) hij pleegde daden of antecedenten die beschouwd kunnen worden als:

— ofwel a) een misdaad of wanbedrijf die de fysieke of psychische integriteit van derden aantast of bedreigt;

— ofwel b) onderrichtingen of opleidingen voor de vervaardiging of het gebruik van explosieven, vuurwapens of andere wapens of schadelijke of gevaarlijke stoffen, dan wel voor andere specifieke methoden en technieken nuttig voor het plegen van terroristische misdrijven bedoeld in artikel 137 van het Strafwetboek;

— ofwel c) bewuste handelingen die als materiële steun voor een terroristische/extremistische organisatie of netwerk gelden;

— ofwel d) feiten die door hun aard wijzen op een verontrustend veiligheidsbewustzijn in hoofde van de betrokkene.

De P.G.E. is een natuurlijke persoon die een aanknopingspunt heeft met België. Het kan hier gaan om een juridisch of feitelijk aanknopingspunt. Voorbeelden van een juridisch aanknopingspunt zijn het hebben van de Belgische nationaliteit of een verblijfsrecht in België. De

également avoir un lien d'ordre factuel avec la Belgique, par exemple un séjour – légal ou non – en Belgique, un séjour dans une prison belge ou dans une institution belge pour internés, comme cela se fait pour les H.T.F. Il importe de déterminer un lien fondé et durable, qu'il soit d'ordre juridique ou factuel entre l'E.P.V. et la Belgique. Il ne s'agit donc pas d'insérer dans la banque de données commune T.E.R. toute personne ayant un lien extrêmement ténu avec la Belgique (par exemple, une personne qui a résidé seulement quelques semaines en Belgique). Il y a nécessité de maintenir une certaine flexibilité dans l'établissement du lien avec la Belgique. Cette relative flexibilité est encadrée par un double contrôle en termes de validation. Un premier contrôle est effectué par les services de base lorsqu'ils insèrent un E.P.V. vraisemblable dans la banque de données commune Terrorist Fighters (cela signifie généralement qu'une personne en "Pré-enquête" E.P.V. est reprise, bien que parfois une "Proposition d'insertion" soit aussi possible). Un deuxième contrôle est effectué par l'OCAM lors de la validation d'une personne dans la banque de données commune T.E.R.

Le premier critère pour être reconnu comme E.P.V. stipule que le E.P.V. a des conceptions extrémistes qui justifient l'usage de la violence ou de la contrainte comme méthode d'action en Belgique.

La notion d' "extrémisme" qui est utilisée dans le premier critère doit être comprise au sens de l'article 8, 1°, c), de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, à savoir: "les conceptions ou les visées racistes, xénophobes, anarchistes, nationalistes, autoritaires ou totalitaires, qu'elles soient à caractère politique, idéologique, confessionnel ou philosophique, contraires, en théorie ou en pratique, aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux autres fondements de l'État de droit, en ce compris le processus de radicalisation.". Le premier critère prévoit ensuite que les conceptions extrémistes de la personne doivent justifier l'usage de la violence ou de la contrainte comme méthode d'action en Belgique. Pour la notion de "violence ou de force", il est renvoyé à la définition de propagandistes de haine. Les conceptions extrémistes de l'E.P.V. doivent justifier l'usage de la violence ou de la contrainte comme méthode d'action en Belgique. Un partisan de l'État islamique pourra par exemple être repris comme E.P.V. étant donné que ce groupement terroriste propage des actions violentes en Occident et en Belgique. Les E.P.V. sont donc des individus qui ont intériorisé une idéologie, une religion ou une conception politique qui justifie l'usage de la violence comme méthode d'action en Belgique. À cet

betrokken persoon kan ook een feitelijk aanknopingspunt hebben met België, zoals bijvoorbeeld een – al dan niet legaal – verblijf in België, het verblijf in een Belgische gevangenis of in een Belgische inrichting voor geïnterneerden, zoals dit ook geldt voor de H.T.F. Het is belangrijk dat het aanknopingspunt tussen de P.G.E. en België voldoende solide en duurzaam is, of het nu juridisch of feitelijk van aard is. Er zullen dus geen personen opgenomen worden in de gemeenschappelijke gegevensbank T.E.R. die slechts een zeer beperkt aanknopingspunt hebben met België (bijvoorbeeld een persoon die maar enkele weken in België verbleef). Het is noodzakelijk om een zekere flexibiliteit te behouden in het vaststellen van een "aanknopingspunt" met België. Deze relatieve flexibiliteit wordt omkaderd door een dubbele controle op het vlak van validering. Een eerste controle gebeurt door de basisdiensten wanneer zij een vermoedelijke P.G.E. ingeven in de gemeenschappelijke gegevensbank T.E.R. (dit betekent meestal dat een persoon in "Vooronderzoek" P.G.E. wordt opgenomen al is soms een onmiddellijk "Voorstel tot Opname" ook mogelijk). Een tweede controle gebeurt door het OCAD, bij de validering van een persoon in de gemeenschappelijke gegevensbank T.E.R.

Het eerste criterium om als P.G.E. te kunnen opgenomen worden, stelt dat de P.G.E. extremistische opvattingen heeft die het gebruik van geweld of dwang als actiemethode in België legitimeren.

De notie "extremisme" die gebruikt wordt in het eerste criterium moet begrepen worden in de zin van artikel 8, 1°, c), van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, met name: "racistische, xenofobe, anarchistische, nationalistische, autoritaire of totalitaire opvattingen of bedoelingen, ongeacht of ze van politieke, ideologische, confessionele of filosofische aard zijn, die theoretisch of in de praktijk strijdig zijn met de beginselen van de democratie of de mensenrechten, met de goede werking van de democratische instellingen of andere grondslagen van de rechtsstaat. Hieronder wordt ook het radicaliseringsproces begrepen.". Daarnaast stelt het eerste criterium dat de extremistische opvattingen die de persoon heeft, het gebruik van geweld of dwang als actiemethode in België moet legitimeren. Voor de notie "geweld of dwang" wordt verwezen naar de definitie van haatpropagandisten. De extremistische opvattingen van de P.G.E. moeten het gebruik van geweld of dwang als actiemethode in België rechtvaardigen. Zo zal bijvoorbeeld een aanhanger van Islamitische Staat kunnen opgenomen worden als P.G.E., gezien deze terroristische groepering gewelddadige acties propageert in het Westen, en in België. De P.G.E. zijn dus individuen die zich een ideologie, religie of politieke opvatting hebben eigengemaakt die het gebruik van geweld in België als actiemethode rechtvaardigt.

égard, ils ont pour objectif de porter préjudice aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou à d'autres fondements de l'État de droit.

Pour qu'une personne puisse être validée comme E.P.V., elle doit avoir, avec un degré de certitude élevée, des conceptions qui justifient l'usage de la violence pour atteindre les objectifs susmentionnés. Il convient d'analyser le contexte particulier pour faire cette déduction. Une personne qui s'exprime sur les réseaux sociaux comme un fervent partisan de l'État islamique, ne jure que par ce groupement et applaudit aux attentats perpétrés par les partisans de ce groupement en Europe peut être considérée comme ayant des conceptions qui justifient l'usage de la violence dans notre pays pour des raisons idéologiques/religieuses. Il en va de même pour un fervent partisan d'un groupement d'extrême droite réputé pour sa légitimation de la violence ou pour son incitation à recourir à celle-ci contre, par exemple, les demandeurs d'asile ou les musulmans. En tout cas, le degré de certitude doit être élevé quant à l'exactitude de l'information relative aux attitudes et conceptions de la personne concernée. Bien que la définition d'E.P.V. présente de prime abord de fortes similitudes par rapport à celle des H.T.F., il est d'importance considérable de distinguer les deux notions. La catégorie E.P.V. constitue dès lors un complément nécessaire à la catégorie H.T.F., qui reprend des personnes ayant déjà entrepris des actions concrètes pour mettre leurs projets à exécution.

Le deuxième critère pour appartenir à la catégorie d'E.P.V. porte sur l'existence d'indications selon lesquelles la personne concernée a l'intention de recourir à la violence, et ce en conformité avec ses conceptions extrémistes.

Il s'agit d'indications préliminaires révélant une certaine intention dans le chef de la personne concernée, sans qu'il y ait d'indications sérieuses relatives à des actes préparatoires. Dans ce cas, on rejoint en effet le cas du *Homegrown Terrorist Fighter* (H.T.F.), qui se distingue en ce qu'il entreprend déjà des actions spécifiques en vue de concrétiser son intention.

Le fait qu'il existe une certaine intention dans le chef de la personne concernée peut être établi de différentes manières. Il peut s'agir par exemple de menaces spécifiques qui sont adressées par la personne concernée à des tiers (avec ou sans fonction officielle), ou de renseignements indirects recueillis par les services. En tout cas, aucune action matérielle spécifique ne doit encore être présente pour pouvoir parler de l'existence de "l'intention". Toutefois, l'information dont l'on dispose pour conclure qu'il existe une certaine "intention" dans le

Het objectief hierbij is om schade te berokkenen aan de beginselen van de democratie of de mensenrechten, de goede werking van de democratische instellingen of andere grondslagen van de rechtsstaat.

Om als P.G.E. te kunnen worden gevalideerd is het noodzakelijk dat de betrokkene met een grote mate van zekerheid opvattingen bezit die het gebruik van geweld legitimeren om bovenvermelde doeleinden te bereiken. Dit kan uiteraard worden afgeleid uit de specifieke context. Iemand die zich op sociale media uit als een fervente voorstander van Islamitische Staat, dweept met deze groepering en de aanslagen die door aanhangers van deze groepering in Europa worden uitgevoerd, toejuicht, kan geacht worden opvattingen te bezitten die het gebruik van geweld in ons land toelaten omwille van ideologisch/religieuze redenen. Hetzelfde geldt voor een fervente aanhanger van een extreemrechtse groepering die gekend staat voor het legitimeren van of het oproepen tot het gebruik van geweld tegen bijvoorbeeld asielzoekers of moslims. In ieder geval moet er sprake zijn van een grote mate van zekerheid dat de informatie over de attitudes en opvattingen van de betrokkene, correct is. Hoewel de definitie van de P.G.E. op het eerste gezicht sterke gelijkenissen vertoont met de H.T.F., is het van substantieel belang om beiden gescheiden te houden. De categorie P.G.E. vormt een noodzakelijke aanvulling op de categorie H.T.F., waarbij het in geval van deze laatste handelt om personen die al concreet in actie zijn geschoten om hun plannen tot uitvoering te brengen.

Het tweede criterium dat bepaalt wanneer een persoon tot de categorie P.G.E. behoort, heeft betrekking op het feit of de persoon in kwestie de intentie heeft om geweld te gebruiken en dit in relatie met zijn extremistische opvattingen.

Het betreft hier preliminaire aanwijzingen die wijzen op een zekere intentie in hoofde van de betrokkene, zonder dat er sprake is van ernstige aanwijzingen aangaande voorbereidingshandelingen. In dat laatste geval komt men immers terecht in de casus van de *Homegrown Terrorist Fighter* (H.T.F.), die zich onderscheidt doordat hij reeds daadwerkelijk specifieke acties onderneemt om zijn intentie te concretiseren.

Het feit dat er enige intentie bestaat in hoofde van de betrokkene kan op verschillende manieren worden vastgesteld. Zo kan het gaan om specifieke bedreigingen die worden geuit door de betrokkene naar derden toe (al dan met een ambtelijke functie), alsook om indirecte inlichtingen verzameld door de diensten. In ieder geval dienen er nog geen specifieke materiële handelingen aanwezig te zijn om te kunnen spreken van de aanwezigheid van "intentie". Wel is het zo dat de informatie waarover men beschikt om te concluderen dat er enige

chef de la personne concernée, doit être jugée comme étant fiable, afin d'éviter que tout un chacun au sujet duquel circulent des rumeurs concernant une intention potentielle entre en ligne de compte pour une validation comme E.P.V. Il convient de préciser que les indications selon lesquelles la personne concernée a l'intention de recourir à la violence doivent être fiables.

Le troisième critère pour être reconnu comme E.P.V. se compose de trois sous-critères et au moins l'un des trois sous-critères présentés ci-dessous doit être rempli. Il s'agit de facteurs présents dans le chef de la personne concernée et qui augmentent le risque de violence.

Un premier sous-critère concerne les contacts sociaux que la personne concernée a développés et la mesure dans laquelle il existe des liens problématiques avec des individus extrémistes connus par les services. En d'autres termes, si une personne entretient systématiquement des contacts avec d'autres extrémistes et est fortement impliquée dans un tel environnement, cela peut légitimement être considéré comme un facteur de risque supplémentaire. Il peut s'agir de personnes ayant déjà un statut spécifique (H.T.F., P.H., F.T.F.), mais cela ne doit pas nécessairement être le cas, étant donné qu'également des individus sans "statut" ont parfois des conceptions très extrémistes. Les services doivent bien entendu rester vigilants pour s'assurer que la présence dans un environnement radical ne conduise pas automatiquement à la conclusion que la personne concernée partage les mêmes idées.

Un deuxième sous-critère concerne les problèmes psychiques. Il s'agit de la présence ou de l'absence d'un ou de plusieurs problèmes psychiques qui augmentent le risque que survienne un comportement violent (troubles de la personnalité, troubles psychiatriques, trouble lié à une substance). S'il ressort d'éléments existants que la situation clinique de la personne concernée entraîne un risque accru de violence, constatée par exemple par le service psycho-social de la prison, cela doit être pris en compte dans l'évaluation de la menace. Quant à la question de savoir qui évaluera s'il existe des problèmes psychiques et qui est qualifié pour évaluer l'État de santé mentale dans les services de base, les auteurs du présent projet tiennent à souligner qu'ils comprennent la sensibilité de ce critère et qu'ils y ont intégré les garanties nécessaires. Ainsi, les problèmes psychiques doivent toujours être constatés par un professionnel compétent en la matière. L'OCAM se charge ensuite d'évaluer le plus précisément possible le danger émanant de la personne en question. L'OCAM compte à cet effet parmi son personnel une psychologue qui peut formuler un avis professionnel lors de la validation finale d'une personne en tant qu'E.P.V. Comme nous l'avons déjà mentionné,

"intentie" bestaat in hoofde van de betrokkene, moet worden beoordeeld als betrouwbaar, teneinde te voorkomen dat elkeen over wie geruchten circuleren omtrent een mogelijke intentie, in aanmerking zou komen voor een validering als P.G.E. Er moet op gewezen worden dat de aanwijzingen dat de betrokkene de intentie heeft om geweld te gebruiken, betrouwbaar moeten zijn.

Het derde criterium om als P.G.E. te kunnen opgenomen worden, bestaat uit een drietal sub-criteria. Er moet aan minstens een van deze drie hieronder beschreven subcriteria voldaan zijn. Het gaat om factoren die in hoofde van de betrokkene aanwezig zijn en die het risico op geweld verhogen.

Een eerste subcriterium betreft de sociale contacten die de persoon in kwestie heeft uitgebouwd, en de mate waarin er hierbij sprake is van problematische connecties met door de diensten gekende extremistische individuen. Met andere woorden, indien een persoon er op systematische wijze contacten met andere extremisten op nahoudt en zwaar ingebed zit in een dergelijke milieu, dan kan dit terecht worden beschouwd als een bijkomende risicofactor. Het kan gaan om mensen die reeds onder een specifiek statuut staan (H.T.F., H.P., F.T.F.), maar dit hoeft niet noodzakelijk het geval te zijn, gezien ook individuen zonder een "statuut" er soms zéér extremistische opvattingen op nahouden. De diensten moeten er uiteraard over waken zich ervan te vergewissen dat de aanwezigheid in een radicale omgeving, niet automatisch tot de conclusie leidt dat de betrokkene dan ook dezelfde ideeën koestert.

Een tweede subcriterium is de psychische problematiek. Het gaat hierbij over de aan- of afwezigheid van (een) psychische stoornis(sen) die de kans op het optreden van gewelddadig gedrag verhogen (persoonlijkheidsstoornissen, psychiatrische stoornissen, middelenproblematiek). Indien elementen voorradig zijn waaruit blijkt dat de klinische toestand van de betrokkene tot een verhoogd risico op geweldpleging leidt, vastgesteld door bijvoorbeeld de psychosociale dienst van een gevangenis, dan dient dit in de inschatting van de dreiging te worden meegenomen. Wat betreft de vraag wie er zal oordelen of er sprake is van een psychische problematiek, en wie binnen de basisdiensten gekwalificeerd is om de psychische gezondheidstoestand te evalueren, wensen de opstellers van dit ontwerp te benadrukken dat zij de gevoeligheid van dit criterium begrijpen en de nodige waarborgen hebben ingebouwd. Zo moet de psychische gezondheidstoestand steeds vastgesteld worden door een daartoe gekwalificeerde deskundige. Het OCAD gaat hier vervolgens mee aan de slag om het gevaar, dat uitgaat van de persoon in kwestie, zo accuraat mogelijk in te schatten. Het OCAD heeft hiervoor een psychologe in dienst die, bij de finale validering van een persoon als

les services psychosociaux (SPS) de l'Administration pénitentiaire ont également les compétences nécessaires pour évaluer l'État de santé mentale d'une personne. L'OCAM ne doit pas nécessairement toujours recevoir les rapports complets qui décrivent la pathologie mentale de la personne concernée, mais il doit être informé de la pathologie et de la qualité de la personne qui a posé ce diagnostic afin de pouvoir évaluer correctement la menace. Comme précisé précédemment, ce sous-critère ne doit pas être pris en considération de façon isolée. Il s'agit en effet d'un critère cumulatif avec les critères visés à l'article 1, 9°, a) et b), explicités ci-avant et le cas échéant, avec les deux autres sous-critères visés à l'article 1, 9°, c).

Le troisième sous-critère se concentre sur les actes et antécédents spécifiques de la personne concernée et peut également être subdivisé en plusieurs paramètres. On examine notamment les antécédents violents (judiciaires) et les capacités d'une personne. Il se peut que la personne concernée ait déjà été condamnée par le passé pour des infractions violentes ou qu'elle ait suivi des formations spécifiques au maniement des armes ou à la fabrication d'explosifs ou à d'autres méthodes et techniques en vue de commettre des infractions terroristes. De même, la personne concernée peut avoir déjà prouvé qu'elle n'hésite pas à utiliser la violence comme méthode d'action, à la suite de quoi certains "seuils" ont déjà été dépassés. Il peut également arriver que la personne concernée commette ou ait commis des actes qui peuvent être considérés comme apportant un soutien matériel à une organisation ou à un réseau terroriste/extrémiste, par exemple, en soutenant financièrement un tel groupe ou en rendant divers autres services. Ces actes doivent être suffisamment graves et intentionnels pour être repris dans ce critère. L'intention de porter gravement préjudice en apportant un soutien à une organisation ou un réseau terroriste/extrémiste doit être claire.

Enfin, il est également possible que la personne concernée présente des comportements qui impliquent une vigilance anormale à l'égard de la sécurité, par exemple:

- l'utilisation de certaines techniques de contre-surveillance (changer de moyen de circulation au dernier moment, retirer la batterie de son GSM, pas de GSM lors de rencontre,);

- l'utilisation d'un langage codé;

P.G.E. een professioneel advies kan geven. Zoals eerder vermeld, hebben de psychosociale diensten (PSD) binnen het gevangeniswezen eveneens de nodige competentie om iemands psychische gezondheidstoestand te evalueren. Het OCAD moet hiervoor niet noodzakelijk altijd de volledige rapporten waarin het psychische ziektebeeld van de betrokkene wordt beschreven, ontvangen, wel moet het OCAD op de hoogte zijn van het ziektebeeld en van de hoedanigheid van de persoon die de diagnose heeft gesteld om de dreiging correct te kunnen inschatten. Zoals hierboven vermeld, mag dit subcriterium niet op zichzelf worden beschouwd. Het is een cumulatief criterium met de criteria bedoeld in artikel 1, 9°, a) en b), hierboven toegelicht, en, in voorkomend geval, met de twee andere subcriteria bedoeld in artikel 1, 9°, c).

Het derde subcriterium focust op welbepaalde daden en antecedenten die de betrokkene pleegt of heeft gepleegd en valt eveneens op te delen in meerdere parameters. Zo wordt onder meer gekeken naar iemands gewelddadige (gerechtelijke) antecedenten en capaciteiten. Het kan zijn dat de betrokkene in het verleden al veroordeeld werd omwille van gewelddadige misdrijven of dat de betrokkene specifieke opleidingen heeft gevolgd waarin hij geleerd heeft om te gaan met wapens of geschoold is in de productie van explosieven of andere methoden en technieken met het oog op het plegen van terroristische misdrijven. Of de betrokkene heeft al bewezen dat hij of zij er niet voor terugdeinst om geweld te gebruiken als actiemethode, waardoor op die manier zekere "drempels" al zijn overschreden. Ook kan het zijn dat de betrokkene feiten pleegt of pleegde die beschouwd kunnen worden als het leveren van materiële steun voor een terroristische/extremistische organisatie of netwerk, zoals bijvoorbeeld het financieel ondersteunen van een dergelijke groepering, of het leveren van andere hand- en spandiensten. Deze daden dienen voldoende zwaarwichtig te zijn en intentioneel te gebeuren om meegenomen te kunnen worden in dit criterium. De intentie om ernstige schade te berokkenen door steun te verlenen aan een terroristische/extremistische organisatie of netwerk moet duidelijk zijn.

Ten slotte is het eveneens mogelijk dat de betrokken persoon gedrag vertoont dat een abnormale waakzaamheid op het stuk van veiligheid impliceert, bijvoorbeeld:

- het gebruik van bepaalde contra-surveillance-technieken (op het laatste moment van verkeersmiddel wisselen, de batterij uit zijn gsm halen, geen gsm tijdens de ontmoeting, enz.);

- gebruik van codetaal;

- alors qu'elle est connue;, la personne utilise des alias dans les médias sociaux;
- le fait d'effacer son historique de recherche média;
- pratiquer la Taqiyya;
- avoir 10 téléphones ou aucun;
- n'utiliser que des réseaux sociaux très sécurisés;
- avoir 20 caméras / détecteurs autour de chez soi;
- voyager avec des faux papiers;
- ne voyager qu'à partir d'aéroports étrangers;
- utiliser les systèmes *hawallah*/cryptomonnaies pour l'échange d'argent;
- ne parler des dossiers sensibles qu'à l'extérieur.

Il s'agit toutefois de facteurs qui sont présents chez la personne concernée et qui, selon les outils d'évaluation du risque calibrés, augmentent le risque de violence. L'évaluation finale des informations et des renseignements relatifs à ces critères et la décision de valider et de reprendre une personne donnée dans la banque de données commune T.E.R. sont du ressort de l'OCAM et non des services de police.

Le raisonnement qui sous-tend cette catégorie E.P.V. se base sur le fait qu'il s'est avéré indispensable de pouvoir suivre à travers la banque de données commune T.E.R., une fraction d'individus dont les services estiment qu'ils représentent un risque accru de violence, même s'ils ne sont pas encore passés à l'acte. Bien que la définition d'E.P.V. présente de prime abord de fortes similitudes par rapport à celle des H.T.F., il est d'importance considérable de distinguer les deux notions. La catégorie E.P.V. constitue dès lors un complément nécessaire à la catégorie H.T.F., qui reprend des personnes ayant déjà entrepris des actions concrètes pour mettre leurs projets à exécution. Il s'agit d'individus ayant fait des démarches ou entrepris des actes d'exécution afin de commettre un acte terroriste violent. Ces derniers feront *de facto* l'objet d'une enquête judiciaire et dans de nombreux cas également d'une condamnation judiciaire. Compte tenu des exigences élevées qui sont à la base de la validation d'un H.T.F., il s'agit dans presque tous les cas de personnes qui sont arrêtées in extremis dans la mise en exécution d'un projet concret ou de personnes qui sont parvenues à mettre à exécution leurs projets sans avoir été repérées par les services concernés. En ce qui concerne les E.P.V., il n'est pas encore possible d'établir que la personne concernée

- terwijl hij gekend is, gebruikt de persoon aliasen op sociale media;
- het feit dat hij zijn zoekgeschiedenis wist;
- de takiyya beoefenen;
- tien of geen telefoons hebben;
- enkel zeer beveiligde sociale netwerken gebruiken;
- twintig camera's/detectoren rond zich hebben;
- reizen met valse papieren;
- enkel reizen vanuit buitenlandse luchthavens;
- het *hawala*-systeem of cryptomunten gebruiken om geld uit te wisselen;
- enkel buiten over gevoelige dossiers praten.

Het gaat hier echter om factoren die in hoofde van de betrokkene aanwezig zijn en die, volgens geijkte risicotaxatie-instrumenten, het risico op geweld verhogen. De finale evaluatie van de informatie en inlichtingen met betrekking tot die criteria en de beslissing tot validatie en opname van een bepaalde persoon in de gemeenschappelijke gegevensbank T.E.R., ligt bij het OCAD, en niet bij de politiediensten.

De redenering achter deze categorie P.G.E., is dat het noodzakelijk is gebleken om een deel van individuen waarvan de diensten vinden dat er sprake is van een verhoogd risico op geweldpleging, zelfs indien ze nog niet zijn overgegaan tot daden, op te kunnen opvolgen in de gemeenschappelijke gegevensbank T.E.R. Hoewel de definitie van de P.G.E. op het eerste gezicht sterke gelijkenissen vertoont met de H.T.F., is het van substantieel belang om beiden gescheiden te houden. De categorie P.G.E. vormt een noodzakelijke aanvulling op de categorie H.T.F., waarbij het in geval van deze laatste handelt om personen die al concreet in actie zijn geschoten om hun plannen tot uitvoering te brengen. H.T.F. zijn individuen die stappen of uitvoeringshandelingen hebben gezet om een gewelddadige terreurdaad te plegen, wat *de facto* ertoe zal leiden dat zij het voorwerp uitmaken van een gerechtelijk onderzoek en in veel gevallen ook van een gerechtelijke veroordeling. De hoge eisen die aan de basis liggen van een validering van H.T.F. maakt dat het in quasi alle gevallen handelt om personen die in extremis gestopt worden met de uitvoering van een concreet plan, dan wel om personen die erin slaagden hun plannen uit te voeren zonder dat ze werden gedetecteerd door de betrokken diensten. Wat betreft de P.G.E. is het zo dat er nog niet eenduidig kan worden gesteld

se trouve effectivement sur une trajectoire qui conduira inévitablement à un acte terroriste si rien n'est entrepris. Si par contre les critères d'E.P.V. sont remplis, il faut être sur ses gardes. Ces critères sont en grandes lignes les mêmes indicateurs qui sont actuellement à la base des "instruments d'évaluation des risques" reconnus qui sont utilisés pour estimer dans quelle mesure certains individus comportent un risque plus élevé de violence extrémiste. Les indicateurs relatifs aux E.P.V. ne sont donc pas choisis au hasard, mais sont considérés comme étant les éléments principaux à prendre en compte afin de juger s'il s'agit d'un risque accru de violence.

La raison d'être de cette catégorie est donc grâce à un suivi commun et intégral, de dresser les priorités au sein de la fraction du spectre extrémiste qui peut être considérée comme comportant un risque élevé de violence. Il s'agit aussi bien d'individus incarcérés que de personnes en liberté. La priorisation de tels individus implique qu'ils soient repris dans la banque de données commune T.E.R. et qu'il soit examiné en commun et au cas par cas si des mesures doivent être prises et lesquelles en vue de diminuer la menace potentielle émanant de ces individus.

4° Les Personnes condamnées pour terrorisme sont les personnes qui ont un lien avec la Belgique et qui ont été condamnées ou qui ont reçu une décision judiciaire d'internement ou, dans le cas de mineurs, fait l'objet d'une mesure de protection (loi du 8 avril 1965 "relative à la protection de la jeunesse, à la prise en charge des mineurs ayant commis un fait qualifié infraction et à la réparation du dommage causé par ce fait", Vlaamse decreet jeugddelinquentie dd. 15/2/2019 et décret du 18/01/2018 de la Communauté française relatif à la prévention, l'aide et la protection de la jeunesse) pour des infractions terroristes, telles que décrites au Livre II, Titre 1^{er}ter, du Code Pénal (en Belgique) ou des faits qualifiés comme tels ou par une infraction équivalente à l'étranger et à l'égard de qui l'OCAM a estimé que le niveau de la menace qu'elles représentent se définit comme moyen (niveau 2), grave (niveau 3) ou très grave (niveau 4). Il importe d'inclure cette catégorie dans la banque de données commune T.E.R., en vue d'assurer le flux d'information vers tous les services de base et partenaires. De la sorte, tous les acteurs qui doivent assurer un suivi de "Personnes condamnées pour terrorisme" (tels que la DG EPI, les Maisons de Justice, la police, les centres fermés, la VSSE, les Task Forces locales, ...) peuvent être informés sur la base de leurs droits d'accès à propos des personnes concernées, de manière proactive et en temps utile. Concrètement,

dat de betrokkene daadwerkelijk op een traject zit dat onvermijdelijk zal leiden tot een terreurdaad, indien er niet wordt ingegrepen. Wel is het zo dat indien de criteria van P.G.E. vervuld zijn, er een knipperlicht dient aan te gaan. Deze criteria zijn in grote lijnen dezelfde indicatoren die vandaag de dag aan de basis liggen van de geijkte "risico-taxatie instrumenten" die worden gebruikt om in te schatten in welke mate van bepaalde individuen een groter risico op extremistisch geweldpleging uitgaat. De indicatoren met betrekking tot de P.G.E. zijn dus niet uit de lucht gegrepen, maar worden gezien als de belangrijkste elementen die in rekening moeten worden gebracht om te kunnen oordelen of er sprake is van een verhoogd risico op geweldpleging.

De ratio achter deze categorie ligt er derhalve in om via een gemeenschappelijke en integrale opvolging dat deel van het extremistisch spectrum waarvan geacht kan worden dat er een hoog risico op geweldpleging uitgaat, prioriteit te geven. Het gaat hierbij zowel om individuen die zich in de gevangenis bevinden, alsook om personen die zich vrij bewegen. Het prioriteit geven aan dergelijke individuen houdt in dat ze worden opgenomen in de gemeenschappelijke gegevensbank T.E.R. en dat er gemeenschappelijk en geval per geval wordt bekeken of er maatregelen dienen te worden genomen en zo ja, welke, om de potentiële dreiging die van deze individuen uitgaat te verminderen.

4° De Terrorismeveroordeelden zijn de personen die een aanknopingspunt hebben met België en die veroordeeld werden of een gerechtelijke beslissing tot internering kregen, of in het geval van minderjarigen, die een beschermingsmaatregel kregen (wet van 8 april 1965 "betreffende de jeugdbescherming, het ten laste nemen van minderjarigen die een als misdrijf omschreven feit hebben gepleegd en het herstel van de door dit feit veroorzaakte schade", decreet van 15 februari 2019 van de Vlaamse overheid betreffende het jeugddelinquentierecht en decreet van 18 januari 2018 van de Franse Gemeenschap houdende het wetboek van preventie, hulpverlening aan de jeugd en jeugdbescherming) voor terroristische misdrijven zoals bepaald in Boek 2, Titel 1^{ter}, van het Strafwetboek (in België), of voor gelijkaardige inbreuken in het buitenland, en waarvan het niveau van de dreiging dat van hen uitgaat door het OCAD wordt ingeschaald als gemiddeld (niveau 2), ernstig (niveau 3) of zeer ernstig (niveau 4). Het is van belang om deze categorie op te nemen in de gemeenschappelijke gegevensbank T.E.R. om de informatiedoorstroming naar alle basis- en partnerdiensten te verzekeren. Op deze manier worden alle actoren die een opvolging moeten verzekeren van "Terrorismeveroordeelden" (bijvoorbeeld DG EPI, Justitiehuizen, politie, de gesloten asielcentra, de VSSE, de Lokale Task Forces, ...) proactief, op tijd en volledig geïnformeerd over de betrokkene, op basis

des informations peuvent par exemple être échangées à propos de l'évolution de la personne concernée, ses contacts au sein de la prison ainsi que sur les libérations (temporaires) potentielles, ... La collaboration entre les services pourra en outre être davantage coordonnée.

L'OCAM ou les services de base ne peuvent alimenter la banque de données commune avec les données relatives aux condamnations des étrangers à l'étranger ou des Belges condamnés en dehors de l'Union européenne que si l'OCAM ou ces services sont mis en possession de ces données.

5° les propagandistes de haine visent toutes personnes physiques ou morales, des associations de fait ainsi que de l'ensemble des moyens utilisés par ceux-ci, qui ne doivent pas nécessairement avoir la nationalité belge, séjourner en Belgique ou avoir séjourné en Belgique mais qui remplissent les conditions cumulatives suivantes:

a) le propagandiste de haine a pour objectif de porter atteinte aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux autres fondements de l'État de droit. Il n'est pas nécessaire que l'objectif de porter atteinte soit réalisé, la potentialité de cet objectif est suffisante;

b) le propagandiste de haine justifie l'usage de la violence ou de la force (y compris la toutes les formes de violence ou de la force, comme la violence physique et psychique, la violence intra- et extrafamiliale, la violence homophobe, les cyber-attaques, ...) afin de réaliser cet objectif (porter atteinte, en théorie ou en pratique, aux institutions démocratiques ou aux autres fondements de l'État de droit ainsi qu'aux droits de l'homme). Le propagandiste de haine manifeste son intention de porter préjudice ainsi que la justification du recours à la violence ou la force envers une ou plusieurs entités, par le biais d'actions ou de canaux concrets. L'intention doit être extériorisée publiquement au travers par exemple d'une publication;

c) le propagandiste de haine agit dans le but d'exercer une influence radicalisante sur d'autres personnes. Est entendu par-là que le propagandiste de haine souhaite soutenir ou participer à un processus de radicalisation (un processus influençant un individu ou un groupe d'individus de telle sorte que cet individu ou ce groupe d'individus soit mentalement préparé ou disposé à commettre des actes terroristes.);

d) il doit exister un lien avec la Belgique.

van hun toegangsrechten. *In concreto* kan bijvoorbeeld informatie uitgewisseld worden over zijn evolutie, zijn contacten binnen de gevangenis, mogelijke (tijdelijke) invrijheidsstellingen, ... Bovendien zal de onderlinge samenwerking beter afgestemd kunnen worden.

Het OCAD of de basisdiensten kunnen de gemeenschappelijke gegevensbank enkel voeden met gegevens over buitenlanders die in het buitenland veroordeeld zijn of over Belgen die buiten de Europese Unie veroordeeld zijn, indien het OCAD en deze diensten over deze gegevens kunnen beschikken.

5° Met haatpropagandisten worden alle natuurlijke personen, rechtspersonen, feitelijke verenigingen en de door hen aangewende middelen bedoeld, die niet noodzakelijk de Belgische nationaliteit dienen te hebben of in België dienen te verblijven of verbleven te hebben, maar die wel aan de volgende cumulatieve voorwaarden moeten voldoen:

a) de haatpropagandist heeft als doelstelling om schade te berokkenen aan de beginselen van de democratie of de mensenrechten, de goede werking van de democratische instellingen of andere grondslagen van de rechtsstaat. Het is niet noodzakelijk dat de schade zich reeds heeft voorgedaan, de potentiële schade is voldoende;

b) de haatpropagandist rechtvaardigt het gebruik van geweld of dwang (waaronder alle vormen van dwang en geweld worden begrepen, zoals fysiek en psychisch geweld, intra- en extrafamiliaal geweld, homofoob geweld, cyberaanvallen, ...) als actiemethode om deze doelstelling (de schade aan de principes van de democratie, de mensenrechten, aan de goede werking van de democratische instellingen of aan andere fundamenteën van de rechtsstaat) te bereiken. De haatpropagandist geeft blijk van zijn intentie om schade te berokkenen en van de rechtvaardiging tot het gebruik van geweld of dwang ten aanzien van een of meerdere andere entiteiten door middel van concrete acties of kanalen. Deze intentie moet openbaar veruitwendigd worden, bijvoorbeeld door middel van een publicatie;

c) de haatpropagandist handelt met de bedoeling om een radicaliserende invloed uit te oefenen op andere personen. Hiermee wordt bedoeld dat de haatpropagandist een radicaliseringsproces (een proces waarbij een individu of een groep van individuen op dusdanige wijze wordt beïnvloed, dat dit individu of deze groep van individuen mentaal gevormd wordt of bereid is tot het plegen van terroristische handelingen) wenst te ondersteunen of ertoe wil bijdragen;

d) er moet een aanknoping zijn met België.

Il faut noter que l'influence radicalisante est définie comme toute action exercée par une entité dans le but d'initier ou soutenir un processus de radicalisation ou d'y contribuer. La définition du "processus de radicalisation" est celle de l'article 3, 15°, de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité. Il s'agit de tout processus influençant un individu ou un groupe d'individus de telle sorte que cet individu ou ce groupe d'individus soit mentalement préparé ou disposé à commettre des actes de terrorisme. L'influence radicalisante exercée par le propagandiste de haine peut s'exercer en Belgique mais également à l'étranger. Ce qui importe ici est de déterminer un lien fondé, qu'il soit d'ordre juridique et/ou factuel entre le propagandiste de haine et la Belgique. Par exemple, un propagandiste de haine belge manifestant publiquement, en Belgique, son intention de radicaliser d'autres personnes pourrait être repris dans la banque de données commune T.E.R. Le lien juridique retenu dans ce cas serait la nationalité belge du propagandiste de haine. Tel serait également le cas d'un propagandiste de haine étranger qui résiderait en Belgique mais exercerait son influence radicalisante à l'étranger, le lien juridique retenu serait alors son séjour en Belgique. Autre exemple; un propagandiste de haine étranger, résidant à l'étranger et qui diffuserait dans d'autres pays que la Belgique un message à la suite duquel une influence radicalisante s'exercerait spécifiquement en Belgique ou viserait la Belgique, pourrait, lui aussi être repris dans la banque de données commune T.E.R. Dans ce dernier cas, le lien factuel retenu serait l'influence radicalisante exercée effectivement en Belgique. Il ne s'agit donc pas d'insérer dans la banque de données commune T.E.R. toute personne ayant un lien extrêmement ténu avec la Belgique (par exemple, un propagandiste de haine qui aurait résidé quelques semaines en Belgique il y a de nombreuses années). Il y a nécessité de maintenir une certaine flexibilité dans l'établissement du lien avec la Belgique. Cette relative flexibilité est encadrée par un double contrôle en termes de validation. Tout d'abord, dans le cadre de la validation des services impliqués dans la banque de données commune T.E.R., lorsqu'ils y introduisent des entités propagandistes de haine, et ensuite, lors du processus de validation de la personne comme propagandiste de haine dans la banque de données commune T.E.R. par l'OCAM.

Les entités spécifiquement visées par cette catégorie sont des personnes physiques ou morales, des associations de fait (organisations ou groupements sans statut juridique) ayant une influence radicalisante. Sont aussi visés dans la définition de l'entité, les divers moyens utilisés dans le but d'avoir une influence radicalisante (par ex. un site web, des tracts, des messages radio ou télévision, des chaînes de radio ou de télévision,

Er zij op gewezen dat "radicaliserende invloed" wordt gedefinieerd als elke actie gepleegd door een entiteit met als doelstelling om een radicaliseringsproces te initiëren, te ondersteunen of ertoe bij te dragen. De definitie van "radicaliseringsproces" is die van artikel 3, 15°, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst. Het is elk proces waarbij een individu of een groep van individuen op dusdanige wijze wordt beïnvloed, dat dit individu of deze groep van individuen mentaal gevormd wordt of bereid is tot het plegen van terroristische handelingen. De radicaliserende invloed van een haatpropagandist kan worden uitgeoefend in België maar ook in het buitenland. Wat belangrijk is hier is dat het aanknopingspunt tussen de haatpropagandist en België voldoende solide is, of het nu juridisch of feitelijk van aard is. Een Belgische haatpropagandist die openlijk in België zijn intentie om andere personen te radicaliseren, veruitwendigt, kan opgenomen worden in de gemeenschappelijke gegevensbank T.E.R. Het juridisch aanknopingspunt in dit geval is de Belgische nationaliteit van de haatpropagandist. Dit is ook het geval voor een buitenlandse haatpropagandist die verblijft in België maar zijn radicaliserende invloed uitoefent in het buitenland. Het juridische aanknopingspunt zal in dit geval zijn verblijf in België zijn. Ander voorbeeld; een buitenlandse haatpropagandist die in het buitenland verblijft en die in andere landen dan België een boodschap verspreidt, die een bijzonder radicaliserende invloed heeft in België of die België viseert, zou ook kunnen opgenomen worden in de gemeenschappelijke gegevensbank T.E.R. In dit laatste geval zal het feitelijk aanknopingspunt de radicaliserende invloed in België zijn. Er zullen dus geen personen opgenomen worden in de gemeenschappelijke gegevensbank T.E.R. die slechts een zeer beperkt aanknopingspunt hebben met België (bijvoorbeeld een haatpropagandist die maar enkele weken in België verbleef jaren geleden). Het is noodzakelijk om een zeker flexibiliteit te behouden in het vaststellen van een "aanknopingspunt" met België. Deze relatieve flexibiliteit wordt omkaderd door een dubbele controle op het vlak van validering. Een eerste controle gebeurt door de partnerdiensten wanneer zij een potentiële haatpropagandist ingeven in de gemeenschappelijke gegevensbank T.E.R. Een tweede controle gebeurt door het OCAD, bij validering van een persoon als haatpropagandist in de gemeenschappelijke gegevensbank T.E.R.

De entiteiten die specifiek door deze categorie worden geviséerd zijn natuurlijke personen of rechtspersonen, en feitelijke verenigingen (organisaties of groeperingen zonder juridisch statuut) die een radicaliserende invloed hebben. De verschillende middelen die zij aanwenden met als doel een radicaliserende invloed uit te oefenen (bijv. een website, traktaat, radio- of televisiebericht of -zender, culturele of propagandacentra, lokalen, enz.)

des centres de propagandes ou culturels, des locaux, etc.). La potentiële influence radicalisante des entités en question consiste en un processus de radicalisation, qui va bien souvent de pair avec un phénomène d'extrémisme dans le chef de ces entités. Ce processus de radicalisation, tel qu'explicité dans l'article 3, 15°, de la loi organique des services de renseignement et de sécurité du 30 novembre 1998, se définit comme suit: il s'agit d'un processus influençant un individu ou un groupe d'individus de telle sorte que cet individu ou ce groupe d'individus soit mentalement préparé ou disposé à commettre des actes de terrorisme. Enfin, l'entité doit être active en Belgique ou développer des activités, par divers moyens, dont les effets radicalisants sont perceptibles dans notre pays.

4) Entité en pré-enquête

Les entités en pré-enquête sont les personnes physiques majeures ou mineures de douze ans et plus, les personnes morales ou associations de fait, ainsi que l'ensemble des moyens utilisés par celles-ci qui sont dans une situation nécessitant un suivi en raison d'indices permettant de conclure qu'elles puissent se trouver dans l'une des situations décrites à l'article 2, 7°, 8°, 9° ou 11° et qui devra être établie. Il s'agit donc d'une situation temporaire à l'issue de laquelle cette entité sera ou non maintenue dans la banque de données commune T.E.R.

Vu la nature des critères visés, la pré-enquête n'est pas prévue pour la catégorie "Personnes condamnées pour terrorisme". Les personnes à l'égard desquelles l'OCAM a estimé que le niveau de la menace qu'elles représentent se définit comme faible (niveau 1) ne sont dès lors pas reprises dans la banque de données commune, comme elles ne requièrent pas ou plus de suivi.

L'objectif est de pouvoir couvrir le cas des personnes pour lesquelles un service de base doit alimenter la banque de données commune T.E.R. en enregistrant la personne parce qu'elle correspond manifestement à l'une des situations décrites. Néanmoins, le service de base doit encore pouvoir solliciter d'autres services pour confirmer la situation exacte de l'entité concernée (validation à son niveau) avant de la proposer au responsable opérationnel (OCAM) pour validation à ce second niveau.

En effet, le but de cette période de "pré-enquête" est de permettre la collecte temporaire (au maximum six mois), mais centralisée dans un seul système de traitement, de données et d'informations qui pourront ou non justifier une validation de l'entité concernée en tant que *foreign terrorist fighter*, *homegrown terrorist fighter*, extrémiste potentiellement violent ou propagandiste de

worden eveneens beoogd. De potentiële radicaliserende invloed van de entiteiten waarvan sprake, is een radicaliseringsproces, dat bovendien vaak gepaard gaat met een fenomeen van extremisme in hoofde van deze entiteiten. Dit radicaliseringsproces, zoals vermeld in artikel 3, 15°, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, wordt gedefinieerd als volgt: het gaat om een proces waarbij een individu of een groep van individuen op dusdanige wijze wordt beïnvloed, dat dit individu of deze groep van individuen mentaal gevormd wordt of bereid is tot het plegen van terroristische handelingen. Tot slot moet de entiteit actief zijn in België of activiteiten ontplooiën, aan de hand van verschillende middelen, waarvan de radicaliserende effecten zichtbaar zijn in ons land.

4) Entiteit in vooronderzoek

De entiteiten in vooronderzoek zijn de meerderjarige natuurlijke personen of minderjarige natuurlijke personen van twaalf jaar en ouder, de rechtspersoon of feitelijke verenigingen, alsook alle de door hen aangewende middelen, die zich in een – te funderen – situatie bevinden die een opvolging vereist vanwege aanwijzingen op basis waarvan kan worden besloten dat zij zich in een van de in artikel 2, 7°, 8°, 9° of 11° beschreven situaties bevinden. Het betreft bijgevolg een tijdelijke situatie. Na afloop ervan zal deze entiteit al dan niet in de gemeenschappelijke gegevensbank T.E.R. geregistreerd blijven.

Er wordt, gezien de aard van de criteria, niet in een vooronderzoek voorzien voor de categorie van "terrorisme veroorzakers". De personen ten aanzien van wie het dreigingsniveau door het OCAD werd beschouwd als laag (niveau 1) worden dus niet opgenomen in de gemeenschappelijke gegevensbank, aangezien zij geen opvolging (meer) behoeven.

Het doel is om de personen mee in rekening te kunnen nemen voor wie een basisdienst de gemeenschappelijke gegevensbank T.E.R. moet voeden door de persoon te registreren omdat hij duidelijk beantwoordt aan een van de beschreven situaties. Niettemin moet de basisdienst nog op andere diensten een beroep kunnen doen om de exacte situatie van de betrokkene te bevestigen (validering op zijn niveau) alvorens omtrent deze entiteit een voorstel te kunnen doen aan de operationeel verantwoordelijke (OCAD) voor validering op dit tweede niveau.

Het doel van die periode van "vooronderzoek" is namelijk tijdelijk (maximaal zes maanden) maar gecentraliseerd in een enkel verwerkingssysteem, gegevens en informatie te kunnen inzamelen die al dan niet een validering van de betrokken entiteit als *foreign terrorist fighter*, *homegrown terrorist fighter*, potentieel gewelddadige extremist of haatpropagandist zullen onderbouwen

haine (phase d'enrichissement). Au plus tard à l'issue de cette période, sur la base des informations/renseignements disponibles, l'OCAM évaluera si les critères légaux sont rencontrés ou non. S'ils ne sont pas rencontrés, l'entité en pré-enquête sera automatiquement supprimée.

Les services de base doivent pouvoir faire appel à d'autres services pour apporter des données concernant la situation exacte de l'entité concernée (et ensuite valider son enregistrement – validation de premier niveau) avant de pouvoir proposer à l'OCAM une validation de cette entité (validation de deuxième niveau). Illustrons ce propos: les services psychosociaux (SPS) au sein des prisons, qui ne font pas partie des services de base ont par exemple une vue précise des conceptions et de l'État de santé psychologique des détenus, il est dès lors nécessaire qu'ils puissent partager des données sur les personnes en pré-enquête E.P.V. par exemple.

L'intérêt d'une banque de données commune est que chaque service apporte les données dont il dispose pour permettre au service de base qui a originellement enregistré l'entité d'assurer sa responsabilité quant à la complétude des données. Dans ce contexte, il faut effectivement donner accès à tous les services concernés qui peuvent fournir des informations et des renseignements nécessaires pour réaliser à l'issue de la période de pré-enquête cette évaluation en deux étapes.

Il va de soi que les services qui ont accès à la banque de données commune T.E.R. savent aussi que l'entité est uniquement en pré-enquête.

Pendant la phase de pré-enquête, l'entité peut être discutée en TFL mais elle ne fait pas l'objet de propositions de mesures de suivi par les TFL. Chaque service ou autorité reste cependant compétent, dans le cadre de ses missions légales, pour prendre les mesures qu'il estime adéquates vis-à-vis de ces entités en pré-enquête.

En ce qui concerne la communication des données de ces entités en pré-enquête à des autorités (par exemple, sous la forme de listes de noms), l'article 25, § 2, contient des garanties concernant la diffusion de listes contenant des données à caractère personnel de la banque de données commune T.E.R. Cet article dispose que:

“La communication par un service de base, sous forme de listes, de données à caractère personnel ou d'informations extraites des cartes d'information, à d'autres

(verrijkingsfase). Uiterlijk na afloop ervan zal het OCAD, op basis van de beschikbare informatie/inlichtingen, evalueren of de wettelijke criteria al dan niet vervuld zijn. Indien deze niet vervuld zijn, zal de entiteit in vooronderzoek automatisch gewist worden.

De basisdiensten moeten op andere diensten beroep kunnen doen om gegevens met betrekking tot de exacte situatie van de betrokkene toe te voegen (en de registratie vervolgens te valideren – validering op het eerste niveau) alvorens omtrent deze persoon een voorstel te kunnen doen aan het OCAD voor een validering van deze entiteit (validering op dit tweede niveau). Een voorbeeld: de psychosociale diensten van de gevangenen (PSD's), die geen basisdiensten zijn, hebben een goed zicht op de opvattingen en psychische gezondheidstoestand van de gedetineerden. Het is dus noodzakelijk dat zij informatie kunnen delen over de personen die in vooronderzoek P.G.E. staan, bijvoorbeeld.

Het belang van een gemeenschappelijke gegevensbank bestaat erin dat elke dienst de gegevens aanbrengt waarover hij beschikt om het aan de basisdienst die de entiteit oorspronkelijk heeft geregistreerd, mogelijk te maken zijn verantwoordelijkheid op het vlak van de volledigheid van de gegevens te verzekeren. In deze context moet men wel degelijk toegang verlenen aan alle betrokken diensten die informatie en inlichtingen kunnen aanreiken die noodzakelijk zijn om tijdens de periode van het vooronderzoek deze evaluatie in twee fasen te kunnen doen.

Uiteraard weten de diensten die toegang hebben tot de gegevensbank T.E.R. dat de entiteit enkel in vooronderzoek is staat.

In de fase van het vooronderzoek kan de entiteit besproken worden in de LTF, maar de LTF's stellen geen opvolgingsmaatregelen voor. Elke dienst of overheid blijft in het kader van zijn of haar wettelijke opdrachten evenwel bevoegd om ten aanzien van die entiteiten in vooronderzoek de maatregelen te nemen die hij of zij het meest gepast acht.

Wat betreft de mededeling van de gegevens van die entiteiten in vooronderzoek aan instanties (bijvoorbeeld in de vorm van namenlijsten), bevat artikel 25, § 2, waarborgen voor het verspreiden van lijsten met persoonsgegevens uit de gemeenschappelijke gegevensbank T.E.R. Dit artikel bepaalt het volgende:

“De mededeling aan andere diensten of instellingen door de basisdienst van persoonsgegevens of informatie gehaald uit de informatiekaarten, onder de vorm van

services ou institutions, n'est pas autorisée, sauf dans les cas prévus à l'article 23. Les listes ne peuvent être communiquées qu'aux autorités publiques et services publics. La finalité de la liste s'inscrit dans les missions légales du destinataire et est précisée et communiquée au destinataire de celle-ci. L'utilisation de la liste n'est autorisée que dans le cadre de la finalité précisée. Les listes ne peuvent pas être conservées pour une durée excédant celle nécessaire à la réalisation de la finalité pour laquelle elles sont obtenues.”

Seules les données à caractère personnel et le informations extraites des cartes d'information d'une entité validée (art. 23) peuvent dès lors être transmises, et ce dans des conditions strictes.

Pour les entités en pré-enquête les données ne peuvent donc pas être partagées avec d'autres services ou institutions dans la mesure où elles ne répondent pas aux critères pour être considérées comme une entité. Elles ne font pas l'objet d'une évaluation de la menace ni d'une carte d'information.

Le projet de loi est ensuite plus précis à propos des critères d'enregistrement dans la banque de données T.E.R. liés à l'âge d'une personne physique: les personnes physiques majeures et mineures à partir de douze ans peuvent être enregistrées dans la banque de données commune T.E.R. si elles correspondent aux critères d'enregistrement. Les mineurs de moins de 12 ans ne sont donc pas enregistrés comme entité dans la banque de données commune T.E.R. Pour les mineurs à partir de 12 ans jusqu'à 18 ans inclus, des mesures de protection additionnelles sont en outre prévues. Ainsi, le délai de conservation maximum dans la banque de données commune T.E.R. après le dernier enregistrement d'une donnée ou information dans la fiche de renseignement de l'entité validée n'est pas de 30 ans mais de 15 ans et le responsable opérationnel est tenu d'évaluer la nécessité d'archiver les données le concernant tous les 3 ans minimum et pas tous les 5 ans. Enfin, lors de l'évaluation préalable à la communication de données via une carte d'information, le statut de minorité doit être pris en compte pour évaluer la nécessité de réaliser cette communication. Par ailleurs, eu égard aux préoccupations du délégué aux droits de l'enfant et du commissaire délégué aux droits de l'enfant au sujet de la formation du personnel chargé de traiter des données relatives à des mineurs, une telle formation devra être dispensée à l'attention du personnel concerné, notamment auprès du responsable opérationnel.

lijsten, wordt niet toegestaan, met uitzondering van de gevallen zoals voorzien in artikel 23. De lijsten kunnen enkel meegedeeld worden aan overheidsinstanties en openbare organen. De doelstelling van de lijst kadert binnen de wettelijke opdrachten van de ontvanger en wordt bepaald en meegedeeld aan de ontvanger. Het gebruik van de lijst wordt enkel toegestaan in het kader van deze welbepaalde doelstelling. De lijsten mogen niet langer bewaard worden dan voor de verwezenlijking van de doelstelling waarvoor zij worden verkregen, noodzakelijk is.”

Enkel de persoonsgegevens en informatie gehaald uit de informatiekaarten van een gevalideerde entiteit (art. 23) mogen dus doorgegeven worden, en dit onder strikte voorwaarden.

Voor de entiteiten in vooronderzoek kunnen de gegevens dan ook niet gedeeld worden met andere diensten of instellingen aangezien ze niet beantwoorden aan de criteria om als een entiteit te worden beschouwd. Ze zijn niet het onderwerp van een dreigingsevaluatie of informatiekaart.

Het wetsontwerp schept vervolgens meer duidelijkheid rond de criteria van de opname in de gegevensbank T.E.R. met betrekking tot de leeftijd van een natuurlijke persoon: meerderjarige natuurlijke personen en minderjarige natuurlijke personen vanaf twaalf jaar kunnen in de gemeenschappelijke gegevensbank T.E.R. worden opgenomen als ze voldoen aan de opnamecriteria. Minderjarigen jonger dan twaalf jaar worden dus niet als entiteit in de gemeenschappelijke gegevensbank T.E.R. opgenomen. Voor minderjarigen van twaalf tot en met achttien jaar wordt er bovendien in extra beschermingsmaatregelen voorzien. Zo bedraagt de maximale bewaringstermijn in de gemeenschappelijke gegevensbank T.E.R. na de laatste registratie van een gegeven of informatie in de inlichtingenfiche van de gevalideerde entiteit niet dertig maar vijftien jaar en moet de operationeel verantwoordelijke de noodzakelijkheid om de gegevens te archiveren die op hem betrekking hebben, minimaal om de drie jaar en niet om de vijf jaar evalueren. Tot slot is het zo dat bij de evaluatie vóór de mededeling van gegevens via een informatiekaart rekening moet worden gehouden met het statuut van minderjarige om te beoordelen of het noodzakelijk is om die mededeling te doen. Gezien de bezorgdheden van de afgevaardigde voor de rechten van het kind en de kinderrechtencommissaris met betrekking tot de opleiding van het personeel dat belast is met de werking van de gegevens van minderjarigen, moet er bovendien een dergelijke opleiding worden georganiseerd voor het betrokken personeel, inzonderheid voor de operationeel verantwoordelijke.

Le seuil de douze ans a été choisi car il s'agit d'un âge pivot repris dans diverses législations.

En effet, il s'agit de l'âge à partir duquel des mesures peuvent être prises à l'égard de mineurs suspectés d'avoir commis un fait qualifié infraction. Avant cet âge, on privilégie le renvoi vers l'aide aux mineurs en danger et on ne peut en tout cas pas placer l'enfant sur la base du fait qualifié infraction (art. 37, § 2, de la loi du 8 avril 1965 relative à la protection de la jeunesse, à la prise en charge des mineurs ayant commis un fait qualifié infraction et à la réparation du dommage causé par ce fait).

En ce qui concerne la Flandre, le décret du 15 février 2019 sur le droit en matière de délinquance juvénile est entré en vigueur le 1^{er} septembre 2019. Ce décret introduit une présomption irréfragable de non-responsabilité pour un mineur de moins de 12 ans qui a commis un délit de mineur. Les faits, actes ou négligences dont cette personne est suspectée peuvent uniquement donner lieu à son renvoi vers les services d'aide à la jeunesse conformément au décret du 12 juillet 2013 relatif à l'aide intégrale à la jeunesse.

En Communauté française aussi l'âge de 12 ans est utilisé comme âge pivot pour prendre des mesures à l'encontre d'un mineur qui a commis des faits qualifiés infractions (FQI). Sauf la réprimande, aucune autre mesure n'est possible pour un mineur FQI de moins de 12 ans. Toutes les mesures (par ex. placement, prestation éducative d'intérêt général, offre restauratrice, ...) ne sont donc uniquement possibles à partir de 12 ans. L'âge de 14 ans est utilisé comme âge pivot pour le placement en IPPJ même si le placement à partir de 12 ans est possible sous certaines conditions (gravement porté atteinte à la vie/santé d'autrui et comportement particulièrement dangereux). (Décret du 18 janvier 2018 de la Communauté française relatif à la prévention, l'aide et la protection de la jeunesse.)

Par ailleurs, 12 ans est l'âge à partir duquel un enfant peut être associé dans diverses procédures le concernant. Par exemples, il doit donner son consentement à son adoption (art. 348-1 du Code civil), il doit être cité à comparaître devant le tribunal de la jeunesse en cas de procédure de mineur en danger ou de mineur poursuivi du chef d'un fait qualifié infraction (art. 46 de la loi du 8 avril 1965 relative à la protection de la jeunesse, à la prise en charge des mineurs ayant commis un fait qualifié infraction et à la réparation du dommage causé

Er werd geopteerd voor de ondergrens van twaalf jaar omdat dit een spilleeftijd die in verschillende wetgevingen wordt gehanteerd.

Vanaf die leeftijd kunnen immers maatregelen worden genomen ten aanzien van minderjarigen die verdacht worden van het plegen van een als misdrijf omschreven feit. Vóór die leeftijd wordt de voorkeur gegeven aan doorverwijzing naar hulpverlening aan minderjarigen in gevaar, en kan men het kind alleszins niet plaatsen op grond van het als misdrijf omschreven feit (art. 37, § 2, van de wet van 8 april 1965 betreffende de jeugdbescherming, het ten laste nemen van minderjarigen die een als misdrijf omschreven feit hebben gepleegd en het herstel van de door dit feit veroorzaakte schade).

Voor Vlaanderen is op 1 september 2019 het decreet jeugddelinquentierecht dd. 15 februari 2019 in werking getreden. Dit decreet voert een onweerlegbaar vermoeden van niet-verantwoordelijkheid in voor een minderjarige jonger dan twaalf die een jeugddelict gepleegd heeft. De daden, handelingen of nalatigheid waarvan deze persoon wordt verdacht kunnen enkel aanleiding geven tot verwijzing naar de jeugdhulpverlening conform het decreet van 12 juli 2013 betreffende de integrale jeugdhulp.

In de Franse Gemeenschap wordt ook de leeftijd van twaalf jaar gebruikt als spilleeftijd om maatregelen te nemen jegens een minderjarige die als misdrijf omschreven feiten (MOF) heeft gepleegd. Buiten de berisping is geen andere maatregel mogelijk voor een minderjarige MOF die jonger is dan twaalf jaar. Alle maatregelen (bijvoorbeeld plaatsing, prestatie van opvoedkundige aard en van algemeen nut, herstelrechtelijk aanbod, enz.) zijn dan ook enkel mogelijk vanaf twaalf jaar. De leeftijd van veertien jaar wordt gebruikt als spilleeftijd voor de plaatsing in gemeenschapsinstellingen voor jeugdbescherming zelfs indien de plaatsing mogelijk is vanaf twaalf jaar onder bepaalde voorwaarden (ernstige aanslag gepleegd op het leven of op de gezondheid van een persoon en uitzonderlijk gevaarlijk gedrag). (Decreet van 18 januari 2018 van de Franse Gemeenschap houdende het wetboek van preventie, hulpverlening aan de jeugd en jeugdbescherming.)

Overigens geldt twaalf jaar als de leeftijd vanaf wanneer een kind kan betrokken worden bij diverse procedures die het aanbelangen. Zo moet het kind bijvoorbeeld toestemmen in zijn adoptie (art. 348-1 van het Burgerlijk Wetboek), het moet gedagvaard worden om te verschijnen voor de jeugdrechtbank ingeval van procedure van minderjarige in gevaar of van minderjarige die wordt vervolgd wegens een als misdrijf omschreven feit (art. 46 van de wet van 8 april 1965 betreffende de jeugdbescherming, het ten laste nemen van minderjarigen die een als misdrijf

par ce fait), ou encore il doit être informé de son droit d'être entendu par le tribunal de la famille dans les procédures relatives à l'autorité parentale (art. 1004/1 du Code judiciaire).

Au niveau international, le Comité des droits de l'enfant (chargé de surveiller l'application par les États de la Convention internationale des droits de l'enfant) a été très clair dans ses observations n° 10 (2017) relatives aux droits de l'enfant dans le système de justice pour mineurs.

Il précise ce qui suit (n° 32, page 54): "L'article 4 des Règles de Beijing prescrit, dans les systèmes juridiques qui reconnaissent la notion de seuil de responsabilité pénale, de ne pas fixer ce seuil trop bas eu égard aux problèmes de maturité affective, psychologique et intellectuelle. Conformément à cette règle, le Comité a recommandé à des États parties de ne pas fixer à un niveau trop bas l'âge minimum de la responsabilité pénale ou bien de relever cet âge minimum, là où il est trop faible, pour le porter à un niveau acceptable sur le plan international. Il ressort de ces recommandations que le Comité considère comme inacceptable sur le plan international de fixer l'âge minimum de la responsabilité pénale en dessous de 12 ans. Des États parties sont encouragés à relever l'âge trop bas de la responsabilité pénale pour le porter à 12 ans, âge qui constitue un minimum absolu, et à continuer de le relever progressivement".

À cet égard, le Conseil d'État, dans son avis 73.442/2 du 7 juin 2023 a indiqué que "La différence de traitement entre les mineurs selon qu'ils ont atteint ou non l'âge de douze ans semble raisonnablement justifiée en l'espèce au regard de la jurisprudence de la Cour constitutionnelle étant donné que le législateur peut en principe, pour fixer l'âge à partir duquel des données à caractère personnel peuvent être traitées dans un instrument tel que la banque de données commune T.E.R., s'inspirer de l'âge de douze ans qui est fixé dans les lois précitées."

Le Délégué aux droits de l'enfant et le Commissaire aux droits de l'enfant se sont quant à eux montrés critique sur la possibilité d'enregistrer des enfants de douze ans et plus dans la banque de données commune T.E.R. Il nous semble que ces deux avis abordent la problématique de ces enfants uniquement dans une optique pénale. Or, la banque de données communes, dans le cadre de ces enfants, ne s'inscrit pas uniquement dans

omschreven feit hebben gepleegd en het herstel van de door dit feit veroorzaakte schade), en ook moet het kind ingelicht worden over zijn recht om gehoord te worden door de familierechtbank in de procedures aangaande het ouderlijk gezag (art. 1004/1 van het Gerechtelijk Wetboek).

Op internationaal niveau is het Comité voor de rechten van het kind (dat belast is met het toezicht op de toepassing van het Internationaal Verdrag inzake de Rechten van het Kind vanwege de Staten) zeer stellig geweest in zijn opmerkingen nr. 10 (2017) betreffende de rechten van het kind binnen het rechtssysteem voor minderjarigen.

Het preciseert het volgende (nr. 32, bladzijde 54): "*Rule 4 of the Beijing Rules recommends that the beginning of MACR [minimum age of criminal responsibility] shall not be fixed at too low an age level, bearing in mind the facts of emotional, mental and intellectual maturity. In line with this rule the Committee has recommended States parties not to set a MACR at a too low level and to increase the existing low MACR to an internationally acceptable level. From these recommendations, it can be concluded that a minimum age of criminal responsibility below the age of 12 years is considered by the Committee not to be internationally acceptable. States parties are encouraged to increase their lower MACR to the age of 12 years as the absolute minimum age and to continue to increase it to a higher age level.*"

In dat verband heeft de Raad van State in advies nr. 73.442/2 van 7 juni 2023 aangegeven dat "[h]et verschil in behandeling tussen de minderjarigen onderling naargelang ze al dan niet de leeftijd van twaalf jaar hebben bereikt, [...] in casu ten aanzien van de rechtspraak van het Grondwettelijk Hof redelijkerwijze verantwoord [lijkt], aangezien de wetgever bij het vaststellen van de minimumleeftijd van personen wier persoonsgegevens mogen worden verwerkt in een instrument zoals de gemeenschappelijke gegevensbank T.E.R., zich in principe kan laten leiden door de leeftijd van twaalf jaar die in de voornoemde wetten wordt vastgesteld."

De afgevaardigde voor de rechten van het kind en de kinderrechtencommissaris zijn dan weer kritisch over de mogelijkheid om kinderen van twaalf jaar en ouder te registreren in de gemeenschappelijk gegevensbank T.E.R. Het lijkt ons dat die twee adviezen de kwestie van die kinderen enkel vanuit een strafrechtelijk standpunt behandelen. In het kader van die kinderen past de gemeenschappelijke gegevensbank niet alleen in dit

cette perspective car il y a un aspect administratif et de suivi à prendre en considération également.

Dans son avis n° 97/2023 du 16 juin 2023, l'Autorité de protection des données a également indiqué que "le traitement des données à caractère personnel des enfants mineurs de certaines entités outrepassa les finalités de l'enregistrement dans une banque de données accessible à des services dont les missions sont autres que celles des services de renseignement." (§ 105). Il faut néanmoins préciser que le traitement de données de ces enfants n'est pas un traitement "au cas où", comme le suggère l'Autorité de protection des données. En effet, ces données sont au contraire utilisées dans l'intérêt de ces mineurs, pour les accompagner dans une démarche préventive. À titre d'exemple, un enfant d'une entité avait été placé dans une école où le risque de radicalisation était très élevé. L'information officer est intervenu pour qu'il fréquente un autre établissement scolaire et ce, dans l'intérêt de cet enfant.

Pour répondre à ces préoccupations, une nouvelle finalité a été ajoutée à la banque de données commune T.E.R. À ce sujet, il est renvoyé aux commentaires de l'article 5 ci-dessous.

Le concept d'entité, reprend également, outre toute personne physique ou morale ou association de fait, les moyens utilisés. Ces moyens devant être entendus comme vecteurs de radicalisation. Il est parfois difficile au début d'une enquête d'identifier l'entité en tant que personne physique ou morale ou association de fait. Souvent, il sera plus aisé d'identifier le moyen utilisé (site Internet, radio, presse, etc.). Dans ce cas, les moyens doivent être repris dans la banque de données commune T.E.R. Le suivi des moyens utilisés repris dans la banque de données permet alors de prendre, le cas échéant, les mesures adéquates.

Dans son avis 73.442/2 du 7 juin 2023, le Conseil d'État estime que lorsque le projet "entend étendre la définition d'"entité" à celle des "moyens utilisés", il s'agit davantage de viser des catégories de données que des catégories de personnes ou d'associations en tant que telles. Compte tenu de ce constat, la notion de "moyens utilisés" trouverait mieux sa place dans l'article 6 de l'avant-projet, où elle serait alors précisée, au même titre que le sont les autres catégories de données qui y sont déjà visées et compte tenu des particularités qui entourent cette notion, ainsi que cela ressort du commentaire de la disposition". Cette interprétation n'est toutefois pas correcte. En effet, les moyens utilisés ne sont pas forcément reliés à une personne et ne constituent dès lors pas une donnée à caractère personnel.

perspectief, want er moeten eveneens een administratief aspect en een aspect van opvolging in aanmerking worden genomen.

In advies nr. 97/2023 van 16 juni 2023 heeft de Gegevensbeschermingsautoriteit eveneens aangegeven dat "de verwerking van persoonsgegevens van minderjarige kinderen van bepaalde entiteiten [...] de doeleinden [overstijgt] van registratie in een gegevensbank die toegankelijk is voor diensten die andere taken hebben dan die van de inlichtingendiensten". (§ 105). Er moet niettemin worden verduidelijkt dat de verwerking van de gegevens van die kinderen geen verwerking is "voor het geval dat", zoals de Gegevensbeschermingsautoriteit suggereert. In tegendeel, die gegevens worden immers gebruikt in het belang van die minderjarigen om ze te begeleiden bij een preventieve stap. Ter illustratie: een kind van een entiteit werd in een school geplaatst waar het risico op radicalisering zeer hoog was. De information officer is opgetreden zodat het kind naar een andere onderwijsinstelling ging, zulks in het belang van het kind.

Om aan die bezorgdheden tegemoet te komen werd er een nieuw doeleinde aan de gemeenschappelijke gegevensbank T.E.R. toegevoegd. Daarvoor wordt verwezen naar de toelichting bij artikel 5.

Het begrip "entiteit" herneemt, behalve elke natuurlijke persoon of rechtspersoon of feitelijke vereniging, ook de middelen die aangewend worden. Deze middelen moeten worden opgevat als vectoren van radicalisering. Het is bij het begin van een onderzoek echter soms moeilijk om de entiteit te identificeren als een natuurlijke persoon, een rechtspersoon of als feitelijke vereniging. Het identificeren van het gebruikte middel (website, radio, pers, ...) is vaak eenvoudiger. In dit geval moeten de middelen zelf opgenomen worden in de gemeenschappelijke gegevensbank T.E.R. De opvolging van de aangewende middelen hernomen in de gegevensbank laat toe om desgewenst de gepaste maatregelen te nemen.

In advies nr. 73.442/2 van 7 juni 2023 oordeelt de Raad van State dat wanneer het ontwerp "de definitie van "entiteit" wil uitbreiden tot de definitie van "aangewende middelen", [...] het echter veeleer [gaat] om categorieën van gegevens dan om categorieën van personen of van verenigingen als zodanig. Gelet op die vaststelling hoort het begrip "aangewende middelen" veeleer thuis in artikel 6 van het voorontwerp, waar het dan zou moeten worden verduidelijkt, net zoals het geval is met de andere categorieën van gegevens die daar reeds worden vermeld, en rekening houdend met de bijzondere kenmerken van dat begrip, zoals blijkt uit de bespreking van de bepaling". Die interpretatie is echter niet correct. De aangewende middelen zijn immers niet noodzakelijkerwijs gelinkt aan een persoon en vormen

C'est le cas par exemple, lorsque de la propagande est véhiculée par certaines radios mais dont l'auteur n'a pas pu être identifié.

Les enregistrements dans la banque de données commune T.E.R. s'effectuent sur la base de critères objectifs. Il y a lieu de respecter des critères clairs, ancrés légalement, pour effectuer un enregistrement dans la banque de données commune T.E.R. N'importe quelle entité n'y figure pas, pour n'importe quel motif. Nous vivons dans un État de droit: on peut être radical, la liberté d'expression est la règle. Tous les salafistes et toutes les personnes nourrissant des sympathies d'extrême droite ou d'extrême gauche ne figurent pas dans la banque de données commune T.E.R. Ce n'est qu'en cas d'indices qu'une personne représente une menace pour la sécurité nationale que celle-ci y figurera. Il faut en outre préciser que ce n'est pas parce qu'une entité n'est pas reprise dans la banque de données commune que celle-ci ne constitue pas un danger pour la sécurité nationale.

En termes de garantie liée à la conservation des données, il convient de rappeler qu'en application de l'article 7, § 1^{er}, les données à caractère personnel de la banque de données commune T.E.R. sont archivées dès que les finalités visées à l'article 5, alinéa 2, ne sont plus rencontrées, et au maximum 30 ans après le dernier enregistrement d'une donnée ou information dans la fiche de renseignement de l'entité validée. Le responsable opérationnel examine également tous les cinq ans après le dernier enregistrement si les données à caractère personnel présentent toujours un lien direct avec l'une des finalités de l'article 5, alinéa 2. Si tel n'est pas le cas, par exemple parce que l'analyse de la menace montre de manière constante que la personne ne constitue plus une menace, les données sont archivées. Enfin, le responsable opérationnel contrôle la qualité des données traitées au sein de la banque de données commune T.E.R. et s'assure de leur pertinence au regard des finalités (art. 12, al. 2, 1^o et 6^o). Ainsi dès lors qu'un critère constitutif n'est plus rencontré dans le chef d'une entité validée, cette dernière est archivée.

5) Données à caractère personnel

Cette définition renvoie à l'article 4, 1), du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) et à l'article 26, 1^o, de la loi du 30 juillet 2018 relative à la protection des personnes

dan ook geen persoonsgegevens. Dat is bijvoorbeeld het geval wanneer de propaganda wordt verspreid door bepaalde radio's, maar de auteur ervan niet kan worden geïdentificeerd.

Opnamen in de gemeenschappelijke gegevensbank T.E.R. gebeuren op basis van objectieve criteria. Er zijn duidelijke in de wet verankerde criteria die moeten gevolgd worden voor een opname in de gemeenschappelijke gegevensbank T.E.R. Een entiteit wordt niet om het even welke reden opgenomen. We leven in een rechtsstaat: radicaal zijn mag, de vrijheid van meningsuiting is de regel. Niet alle salafisten en personen met rechtsextremistische of linksextremistische sympathieën worden opgenomen in de gemeenschappelijke gegevensbank T.E.R. Het is pas als er aanwijzingen zijn dat een persoon een gevaar vormt voor de nationale veiligheid, dat deze wordt opgenomen. Ook moet duidelijk worden gemaakt dat het feit dat een entiteit niet in de gemeenschappelijke gegevensbank is opgenomen, niet betekent dat zij geen gevaar vormt voor de nationale veiligheid.

Wat de garanties inzake gegevensbewaring betreft moet erop gewezen worden dat, met toepassing van artikel 7, § 1, de persoonsgegevens van de gemeenschappelijke gegevensbank T.E.R. worden gearchiveerd van zodra de doeleinden onder artikel 5, tweede lid, niet meer worden verwezenlijkt en uiterlijk 30 jaar na de laatste registratie van een gegeven of informatie in de inlichtingenfiche van de gevalideerde entiteit. De operationeel verantwoordelijke onderzoekt ook om de vijf jaar na de laatste registratie of de persoonsgegevens nog steeds direct verband houden met een van de doeleinden van artikel 5, tweede lid. Indien dat niet het geval is, bijvoorbeeld omdat uit de dreigingsanalyse consequent blijkt dat de persoon geen bedreiging meer vormt, worden de gegevens gearchiveerd. Tot slot controleert de operationeel verantwoordelijke de kwaliteit van de in de gemeenschappelijke gegevensbank T.E.R. verwerkte gegevens en vergewist hij zich van de relevantie ervan in verhouding tot de doeleinden (art. 12, tweede lid, 1^o en 6^o). Zodra niet langer voldaan is aan een constitutief criterium ten aanzien van een gevalideerde entiteit, wordt zij bijgevolg gearchiveerd.

5) Persoonsgegevens

Deze definitie verwijst naar artikel 4, 1), van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) en naar artikel 26, 1^o, van de wet van 30 juli 2018 betreffende de

physiques à l'égard des traitements de données à caractère personnel (*Moniteur belge* du 05 septembre 2018), ci-après loi relative à la protection des données. Elle vise ainsi "toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée"); est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale".

Dans la mesure où la banque de données commune T.E.R. ne contient aucune donnée classifiée, il était précisé ici que les données à caractère personnel traitées dans la banque de données commune T.E.R. sont non classifiées au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. Toutefois, suite à l'avis du Comité R du 13 juillet 2023 au sujet des définitions (§ 18), le caractère non classifié des données à caractère personnel traitées dans la banque de données commune T.E.R. est maintenant repris à l'article 6 (cf. *infra*).

6) Informations

Lorsqu'il était question d'échanger des informations, la loi sur la fonction de police citait systématiquement la définition telle qu'elle est reprise dans l'article 2. Les informations sont donc les "informations non classifiées conformément à la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité que les services de base et les services partenaires traitent dans le cadre de leurs missions légales respectives". La définition permet d'alléger le dispositif et de le rendre plus lisible.

7) Banque de données commune T.E.R.

Pour simplifier le texte, lorsqu'on parle de 'banque de données commune T.E.R.', il s'agit de la banque de données commune créée par l'article 3. T.E.R. est l'abréviation de "Terrorisme, Extrémisme, processus de Radicalisation". Le nom "T.E.R." a aussi été pensé dans un souci de cohérence avec la nouvelle stratégie nationale contre le terrorisme et l'extrémisme de 2021 qui remplace le plan d'action radicalisme de 2015 et qui se nomme "Stratégie TER". La banque de données commune T.E.R. est en réalité l'actuelle banque de données commune "Terrorist fighters" et "Propagandistes de haine".

bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (*Belgisch Staatsblad* van 5 september 2018), hierna "wet gegevensbescherming". Ze heeft aldus betrekking op "alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (hierna genoemd "de betrokkene"); als een "geïdentificeerde natuurlijke persoon" wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon".

Aangezien de gemeenschappelijke gegevensbank T.E.R. geen geclassificeerde gegevens bevat, was hier verduidelijkt dat de persoonsgegevens die in de gemeenschappelijke gegevensbank T.E.R. worden verwerkt, niet geclassificeerd zijn in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen. In navolging van het advies van 13 juli 2023 van het Comité I over de definities (§ 18) is de niet-geclassificeerde aard van de verwerkte persoonsgegevens in de gemeenschappelijke gegevensbank T.E.R. nu opgenomen in artikel 6 (cf. *infra*).

6) Informatie

Wanneer er sprake was van informatie-uitwisseling, vermeldde de wet op het politieambt stelselmatig de definitie zoals opgenomen in het artikel 2. Informatie is dus "niet-geclassificeerde informatie overeenkomstig de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen die de basisdiensten en de partnerdiensten verwerken in het kader van hun respectieve wettelijke opdrachten". Aan de hand van de definitie kan de bepaling minder omslachtig en leesbaarder worden gemaakt.

7) Gemeenschappelijke gegevensbank T.E.R.

Ter vereenvoudiging van de tekst wordt de gemeenschappelijke gegevensbank die door het artikel 3 wordt gecreëerd "gemeenschappelijke gegevensbank T.E.R." genoemd. "T.E.R." is de afkorting van "Terrorisme, Extremisme, Radicaliseringproces". De naam "T.E.R." werd tevens bedacht met het oog op coherentie met de nieuwe nationale strategie tegen terrorisme en extremisme van 2021, die het actieplan Radicalisme van 2015 vervangt en "Strategie TER" heet. De gemeenschappelijke gegevensbank T.E.R. bestaat in werkelijkheid uit de huidige gemeenschappelijke gegevensbanken "Terrorist Fighters" en "Haatpropagandisten".

8) Evaluation de la menace

Il s'agit de l'évaluation, au sens de l'article 8, alinéa 1^{er}, 2^o, de la loi du 10 juillet 2006 relative à l'analyse de la menace, effectuée par l'Organe de coordination pour l'analyse de la menace au sujet des entités reprises dans la banque de données commune. L'évaluation de la menace était utilisée à plusieurs reprises dans la loi sur la fonction de police sans être définie. L'évaluation de la menace comprend le statut de l'entité, le niveau de menace de l'entité ainsi que la justification du niveau de menace établi.

9) Fiche de renseignements

Cette définition s'inspire de celle existante dans l'article 1^{er}, 11^o, de l'arrêté royal "TF" et l'article 1^{er}, 14^o, de l'arrêté royal "PH". Elle en reprend le contenu mais elle est adaptée aux définitions introduites par le projet, notamment celle "d'information".

La fiche de renseignement contient l'ensemble des données à caractère personnel et des informations relatives à une entité de la banque de données commune T.E.R. provenant de l'ensemble des services qui l'alimentent, y compris les enquêtes en cours et les techniques spécifiques utilisées.

Une fiche de renseignements sur des entités permet non seulement de pouvoir évaluer la menace potentielle que représentent celles-ci mais surtout d'en assurer un suivi afin d'anticiper et d'empêcher soit de possibles actes terroristes de leur part soit de possibles passages aux actes terroristes par des personnes ou des organisations que ces entités sont parvenues à radicaliser au point de leur faire commettre un acte terroriste.

Cette fiche, évaluée par l'expert en matière d'analyse de la menace qu'est l'OCAM, est amenée à évoluer sans cesse au gré des informations rapportées par les services qui alimentent la banque de données commune T.E.R afin de donner l'information la plus complète et la plus à jour possible.

L'exploitation des données de la fiche de renseignements constitue dès lors un outil précieux quant à la menace que représente une entité et au suivi qu'il convient d'organiser.

10) Carte d'information

Cette définition est celle de l'article 1^{er}, 12^o, de l'arrêté royal "TF" et l'article 1^{er}, 15^o, de l'arrêté royal "PH", adaptée

8) Dreigingevaluatie

Het gaat om de evaluatie in de zin van artikel 8, eerste lid, 2^o, van de wet van 10 juli 2006 betreffende de analyse van de dreiging die het Coördinatieorgaan voor de dreigingsanalyse uitvoert met betrekking tot de entiteiten die zijn opgenomen in de gemeenschappelijke gegevensbank. De evaluatie van de dreiging werd meermaals gebruikt in de wet op het politieambt zonder omschreven te zijn. De evaluatie van de dreiging omvat het statuut van de entiteit, het dreigingsniveau van de entiteit en de motivering voor het vastgestelde dreigingsniveau.

9) Inlichtingenfiche

Deze definitie is geïnspireerd op de definitie in artikel 1, 11^o, van het koninklijk besluit "TF" en artikel 1, 14^o, van het koninklijk besluit "HP". Ze neemt er de inhoud van over, maar die is aangepast aan de definities die door het ontwerp worden ingevoerd, inzonderheid die van "informatie".

De inlichtingenfiche bevat alle persoonsgegevens en informatie met betrekking tot een entiteit van de gemeenschappelijke gegevensbank T.E.R. die afkomstig zijn van alle diensten die haar voeden, met inbegrip van lopende onderzoeken en specifieke gebruikte technieken.

Een inlichtingenfiche over entiteiten maakt het niet alleen mogelijk om de mogelijke dreiging die van hen uitgaat te beoordelen, maar vooral ook om een opvolging van deze entiteiten te verzekeren teneinde te anticiperen op mogelijke terroristische daden van hun kant of mogelijke terroristische daden van personen of organisaties die deze entiteiten dusdanig hebben weten te radicaliseren dat zij een terroristische daad plegen, en deze te voorkomen.

Deze fiche, die door de expert in dreigingsanalyse, OCAD, geëvalueerd werd, is van die aard dat zij onophoudelijk moet evolueren in functie van de informatie die aangevoerd wordt door de diensten die de gemeenschappelijke gegevensbank T.E.R. voeden teneinde zo volledig en actueel mogelijke informatie te geven.

De exploitatie van de gegevens in de inlichtingenfiche is dus een waardevol instrument voor het bepalen van de dreiging die van een entiteit uitgaat en voor de opvolging die georganiseerd moet worden.

10) Informatiekaart

Deze definitie is die van artikel 1, 12^o, van het koninklijk besluit "TF" en artikel 1, 15^o, van het koninklijk besluit

à la terminologie utilisée dans le présent projet pour “information” et “entité”.

Il s'agit de la fiche personnelle d'une entité qui consiste en un extrait de la fiche de renseignements, contenant les données à caractère personnel et informations adéquates, pertinentes et non excessives pour le destinataire, en vue du suivi des entités validées. Les données à caractère personnel et informations sont dès lors strictement limitée au besoin d'en connaître du destinataire. Un suivi approprié à la menace et individualisé à la personne pourra, par conséquent, être mis en œuvre notamment par un ensemble de mesures de sécurité et d'accompagnement spécifiques.

Outre l'évaluation de la menace et les données à caractère personnel (date de naissance, NRN, ...), la carte d'information peut également contenir d'autres informations telles que: les liens avec d'autres entités de la banque de données commune T.E.R, les moyens de communication, les alias, les mesures appliquées.

Les rapports de la “Task force locale” et d'autres documents pertinents peuvent également y être repris.

Le service qui a transmis l'information reprise dans la fiche de renseignement détermine si cette information peut également être reprise dans la carte d'information.

11) à 14) **droit de création, droit de lecture, droit d'écriture et droit d'interrogation**

Une série de nouvelles définitions sont relatives aux types d'accès dont disposent les services de base ou les services partenaires. Un arrêté royal déterminera quel accès sera accordé aux différents services. Plutôt que de parler d'accès direct ou interrogation directe qui sont des termes spécifiques à la loi sur la fonction de police, on parle maintenant de droit de création, droit de lecture, droit d'écriture et droit d'interrogation.

Le droit de création consiste en l'enregistrement d'une nouvelle entité dans la banque de données commune.

Le droit de lecture implique de consulter toutes les données à caractère personnel et des informations de la banque de données commune. Ce droit va toujours de pair avec le droit d'écriture.

Le droit d'écriture consiste à introduire, modifier ou effacer des données à caractère personnel et des informations mises par le service auquel celui qui a ce droit appartient dans la banque de données commune. Il va de pair avec le droit de lecture. Le droit d'écriture

“HP” en is aangepast aan de in dit ontwerp gebruikte terminologie voor “informatie” en “entiteit”.

Het gaat om de persoonsfiche van een entiteit die een uittreksel van de inlichtingenfiche vormt, met de persoonsgegevens en informatie die toereikend, ter zake dienend en niet overmatig zijn voor de bestemming, voor de opvolging van de gevalideerde entiteiten. De persoonsgegevens en informatie zijn dus strikt beperkt tot de behoefte om te kennen van de bestemming. Bijgevolg zal een adequate opvolging van de dreiging en een geïndividualiseerde opvolging van de persoon kunnen worden uitgevoerd, inzonderheid door een geheel van specifieke veiligheidsmaatregelen en begeleidende maatregelen.

Naast de dreigingsevaluatie en persoonsgegevens (geboortedatum, RRN, ...) kan de informatiekaart ook andere informatie bevatten, zoals: links met andere entiteiten van de gemeenschappelijke gegevensbank T.E.R., communicatiemiddelen, aliasen, toegepaste maatregelen.

Ook de verslagen van “de lokale taskforce” en andere relevante documenten kunnen worden opgenomen.

De dienst die de informatie in de inlichtingenfiche heeft doorgegeven, bepaalt of deze informatie ook op de informatiekaart kan worden opgenomen.

11) tot en met 14) **creatierecht, leesrecht, schrijfrecht en vraagrecht**

Een reeks nieuwe definities heeft betrekking op de soorten toegang waarover de basisdiensten of de partnerdiensten beschikken. In een koninklijk besluit zal worden bepaald welke toegang aan de verschillende diensten zal worden toegekend. Er wordt niet langer gesproken van “rechtstreekse toegang” of “rechtstreekse bevraging”, termen die specifiek zijn voor de wet op het politieambt, maar van “creatierecht”, “leesrecht”, “schrijfrecht” en “vraagrecht”.

Het creatierecht bestaat in de inschrijving van een nieuwe entiteit in de gemeenschappelijke gegevensbank.

Het leesrecht impliceert het recht om alle persoonsgegevens en informatie in de gemeenschappelijke gegevensbank geheel of gedeeltelijk te raadplegen. Dit recht gaat steeds gepaard met het schrijfrecht.

Het schrijfrecht bestaat in het invoeren, wijzigen of verwijderen van persoonsgegevens en informatie die door de dienst waartoe diegene met dit recht behoort, in de gemeenschappelijke gegevensbank is ingevoerd. Het gaat gepaard met het leesrecht. Het schrijfrecht kan

ne peut en effet être utilement rempli que, si le service qui doit compléter la banque de données commune T.E.R., avec les données visées à l'article 6 qu'il détient, connaît bien le contexte lié à l'entité et dispose donc d'un droit de lecture.

Enfin, le droit d'interrogation impose de prendre connaissance de l'existence ou non d'une entité dans la banque de données commune et en cas de confirmation de l'existence d'une entité dans la banque de données commune T.E.R., la prise de connaissance de l'évaluation de la menace (cf. *infra* art. 22). Ce droit d'interrogation est donné aux services de l'État qui sont susceptibles de rentrer en contact avec une personne T.E.R., et qui en l'absence de la qualité T.E.R. de la personne, peuvent lui délivrer des documents administratifs lui permettant de s'établir en Belgique, d'exercer une profession rémunérée. Mais ceux-ci ne gèrent pas d'informations visées à l'article 6 du projet de loi et ne doivent donc pas alimenter la banque de données commune T.E.R.

Les droits de lecture, d'écriture et d'interrogation constituent pour les services qui en bénéficient une obligation de respectivement lire les données, les écrire ou d'interroger la banque de données commune. Ainsi, les services qui disposent de ces droits sont tenus de les exercer afin que la banque de données commune constitue un outil dynamique et efficace permettant de contribuer de manière optimale à la prévention et au suivi du terrorisme et de l'extrémisme, lorsqu'il peut mener au terrorisme (cf. art. 18).

15) Autorités de contrôle

Les autorités de contrôle sont clairement définies comme étant l'Organe de contrôle de l'information policière d'une part, et le Comité permanent de contrôle des services de renseignement et de sécurité d'autre part. La loi sur la fonction de police ou les arrêtés royaux, parlaient tantôt "d'organe" ou "d'organe de contrôle", ce qui pouvait porter à confusion notamment avec l'OCAM.

16) Interconnexion

L'article 9 prévoit la possibilité d'établir une interconnexion entre la banque de données commune et différentes banques de données, tel que prévu à l'article 44/4, § 4, de la loi sur la fonction de police. L'interconnexion est un traitement, au moyen de procédés automatisés, par lequel:

— soit les données à caractère personnel et les informations de la banque de données commune sont mises en relation (bidirectionnels) avec des données

namelijk enkel zinvol worden uitgeoefend als de dienst die de gemeenschappelijke gegevensbank T.E.R. moet aanvullen met de gegevens bedoeld in artikel 6 die hij in zijn bezit heeft, terdege op de hoogte is van de context in verband met de entiteit en dus leesrecht heeft.

Het vraagrecht, ten slotte, vereist kennis te nemen van het al dan niet bestaan van een entiteit in de gemeenschappelijke gegevensbank en, in geval van bevestiging van het bestaan van een entiteit in de gemeenschappelijke gegevensbank T.E.R., kennis te nemen van de dreigingsevaluatie (zie *infra* art. 22). Dit vraagrecht wordt verleend aan de diensten van de staat die in contact kunnen komen met een T.E.R-persoon en die bij ontstentenis van de hoedanigheid van T.E.R. van die persoon, hem administratieve documenten kunnen verlenen aan de hand waarvan die zich in België kan vestigen en een bezoldigd beroep kan uitoefenen. Zij beheren evenwel geen informatie zoals bedoeld in artikel 6 van het wetsontwerp en hoeven de gemeenschappelijke gegevensbank T.E.R. bijgevolg niet aan te vullen.

Het leesrecht, het schrijfrecht en het vraagrecht houden voor de diensten die er gebruik van maken de verplichting in om de gegevens respectievelijk te lezen, te schrijven of de gemeenschappelijke gegevensbank te bevragen. De diensten die over deze rechten beschikken, zijn aldus verplicht deze uit te oefenen om van de gemeenschappelijke gegevensbank een dynamisch en doeltreffend instrument te maken dat optimaal bijdraagt tot de voorkoming en de opvolging van terrorisme en extremisme, wanneer dit tot terrorisme kan leiden (cf. art. 18).

15) Toezichthoudende overheden

De toezichthoudende overheden worden duidelijk omschreven als het Controleorgaan op de politionele informatie enerzijds en het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten anderzijds. In de wet op het politieambt en de koninklijke besluiten werd soms gesproken van "orgaan" of "controleorgaan", wat tot verwarring kon leiden, inzonderheid met het OCAD.

16) Koppeling

Artikel 9 voorziet in de mogelijkheid om een koppeling tot stand te brengen tussen de gemeenschappelijke gegevensbank en verschillende gegevensbanken, zoals bepaald in artikel 44/4, § 4, van de wet op het politieambt. De koppeling is een verwerking, via een geautomatiseerde procedés, waarbij:

— ofwel de persoonsgegevens en informatie van de gemeenschappelijke gegevensbank (in de twee richtingen) verbonden worden met persoonsgegevens

à caractère personnel et des informations pertinentes enregistrées dans d'autres banques de données gérées par les services de base ou les services partenaires;

— soit, les données à caractère personnel et les informations pertinentes des banques de données, sources authentiques peuvent être transférées vers la banque de données commune T.E.R.

Les détails liés à cette interconnexion sont explicités à l'article 9.

17) Délégué à la protection des données

Le "délégué à la protection des données" est celui visé à l'article 157/1 de la loi relative à la protection des données. Son rôle est de veiller à la conformité en matière de protection des données dans le cadre de la banque de données commune T.E.R. (cf. *infra*).

CHAPITRE 2

De la banque de données commune T.E.R.

Section 1^{er}

Dispositions générales

À titre préliminaire, il convient d'apporter quelques précisions concernant l'avis de l'Autorité de protection des données au sujet du principe de proportionnalité/minimisation des données (Avis n° 97/2023 du 16 juin 2023, §§ 78 à 82). En ce qui concerne particulièrement l'évaluation des dispositions de la loi sur la fonction de police reprises dans le dispositif, c'est précisément l'objet de l'exercice du présent projet. Les dispositions ont été retirées de la loi sur la fonction de police suite aux recommandations de la Commission d'enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016. Le projet prévoit également une révision des accès des services partenaires sur base du respect des principes d'adéquation, de pertinence et du caractère non excessif. Le caractère proportionnel dépend du type d'accès qui sera octroyé aux services partenaires par le Roi.

Art. 3

L'article 3 crée la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation". Il reprend le principe de l'article 44/2, § 2, de la loi sur la fonction de police.

en relevante informatie die geregistreerd zijn in andere gegevensbanken die door de basisdiensten of de partnerdiensten worden beheerd;

— ofwel de persoonsgegevens en de relevante informatie van de gegevensbanken, authentieke bronnen kunnen worden overgezonden aan de gemeenschappelijke gegevensbank T.E.R.

De details van deze koppeling zijn opgenomen in artikel 9.

17) Functionaris voor gegevensbescherming

De "functionaris voor gegevensbescherming" is diegene die wordt beoogd in artikel 157/1 van de wet gegevensbescherming. Zijn rol is om te waken over de conformiteit op het gebied van gegevensbescherming voor wat betreft de gemeenschappelijke gegevensbank T.E.R. (cf. *infra*).

HOOFDSTUK 2

De gemeenschappelijke gegevensbank T.E.R.

Afdeling 1

Algemene bepalingen

Ter inleiding moeten enkele verduidelijkingen worden aangebracht met betrekking tot het advies van de Gegevensbeschermingsautoriteit over het evenredigheidsbeginsel en het beginsel van minimale gegevensverwerking (advies nr. 97/2023 van 16 juni 2023, §§ 78 tot 82). Het is net de bedoeling van dit ontwerp om inzonderheid de bepalingen van de wet op het politieambt die in het instrument zijn opgenomen te evalueren. Die bepalingen werden uit de wet op het politieambt gehaald op aanbeveling van de parlementaire onderzoekscommissie belast met het onderzoek naar de omstandigheden die hebben geleid tot de terroristische aanslagen van 22 maart 2016. Het ontwerp voorziet eveneens in een herziening van de toegang van de partnerdiensten op basis van de inachtneming van de principes van toereikendheid, relevantie en de niet-bovenmatige aard. Het evenredigheidsbeginsel hangt af van de soort toegang die de Koning toekent aan de partnerdiensten.

Art. 3

In artikel 3 wordt de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" gecreëerd. Het herneemt het beginsel van artikel 44/2, § 2, van de wet op het politieambt.

Dans le cadre de la prévention et de la lutte efficaces contre le terrorisme et l'extrémisme pouvant mener au terrorisme, qui risquent d'affecter gravement la protection des personnes, la sécurité ou la santé publique, différents services publics dont les missions légales concernent directement ou indirectement la lutte contre ces phénomènes, sont amenés à unir leurs efforts et à travailler conjointement chacun dans le cadre de leurs missions légales respectives.

À noter que le traitement visé par l'article 3, alinéa 1^{er} vise tout traitement au sens de l'article 26, 2°, de la loi relative à la protection des données, à savoir "toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction des données."

La banque de données commune T.E.R. répond ainsi à la nécessité de structurer l'ensemble des données à caractère personnel et des informations relatives aux missions de prévention et de suivi du terrorisme et de l'extrémisme, lorsqu'il peut mener au terrorisme, fournies par les services de base et les services partenaires de sorte qu'elles soient retrouvées directement afin d'accomplir les finalités visées à l'article 5, alinéa 2.

Toutefois, il est précisé ici que les données à caractère personnel des enfants mineurs d'un *foreign terrorist fighter* (catégorie 1 ou 3), et qui ne sont pas ou ne peuvent pas être considérés comme *foreign terrorist fighters*, *homegrown terrorist fighters*, extrémistes potentiellement violents, personnes condamnées pour terrorisme ou propagandistes de haine, ne peuvent pas être retrouvées directement dans la banque de données commune T.E.R.

En effet, si leur nom est introduit, ces enfants n'apparaissent toutefois pas dans la banque de données commune T.E.R. Ils sont considérés comme des enfants en danger (cf. *infra* article 5).

Par ailleurs, dans la mesure où la banque de données commune est mise en place par le présent projet, ce dernier ne prévoit plus que les ministres de la Justice et de l'Intérieur ont la compétence d'en créer d'autres en matière de terrorisme. En effet, le texte actuel de la loi sur la fonction de police laisse entendre qu'une ou

In het kader van de doeltreffende voorkoming en bestrijding van terrorisme en extremisme dat tot terrorisme kan leiden, waardoor de bescherming van personen, de openbare veiligheid of de volksgezondheid ernstig in het gedrang kunnen komen, moeten verschillende openbare diensten waarvan de wettelijke opdrachten rechtstreeks of onrechtstreeks betrekking hebben op de bestrijding van die fenomenen, hun krachten bundelen en samenwerken, elk in het kader van hun respectieve wettelijke opdrachten.

Er zij op gewezen dat de in artikel 3, eerste lid, bedoelde verwerking alle verwerkingen in de zin van artikel 26, 2°, van de wet gegevensbescherming omvat, namelijk "een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, bekendmaking door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens."

De gemeenschappelijke gegevensbank T.E.R. beantwoordt dus aan de noodzaak tot het structureren van alle persoonsgegevens en informatie betreffende de opdrachten inzake de voorkoming en de opvolging van terrorisme en extremisme, dat kan leiden tot terrorisme, die aangeleverd worden door de basisdiensten en de partnerdiensten, zodat zij direct worden teruggevonden teneinde de doeleinden bedoeld in artikel 5, tweede lid, te bereiken.

Hier wordt echter gespecificeerd dat de persoonsgegevens van de minderjarige kinderen van een *foreign terrorist fighter* (catégorie 1 of 3), die niet worden beschouwd of niet kunnen worden beschouwd als *foreign terrorist fighters*, *homegrown terrorist fighters*, potentieel gewelddadige extremisten, terrorismeveroordeelden of haatpropagandisten, niet rechtstreeks in de gemeenschappelijke gegevens T.E.R. kunnen worden gevonden.

Wanneer hun naam wordt ingevoerd, verschijnen deze kinderen immers niet in de gemeenschappelijke gegevensbank T.E.R. Ze worden eveneens beschouwd als kinderen die in gevaar verkeren (zie artikel 5 hieronder).

Bovendien, aangezien er bij dit ontwerp een gemeenschappelijke gegevensbank wordt opgezet, voorziet het ontwerp niet meer in de bevoegdheid van de ministers van Justitie en van Binnenlandse Zaken om andere gegevensbanken te creëren op het gebied van terrorisme. De huidige tekst van de wet op het politieambt wekt

plusieurs banques de données communes peuvent être créées. Or, multiplier les banques de données communes en matière de terrorisme, extrémisme et processus de radicalisation est contre-productif et ne remplit pas l'objectif de centralisation de l'information souhaité. En outre, dans les faits, au niveau informatique, comme explicité plus haut, il existe une seule et même banque de données commune pour toutes les catégories de personnes ou entités listées dans les arrêtés royaux du 21 juillet 2016 et du 23 avril 2018 précités. Cette réalité n'empêche bien entendu pas que des règles de gestion spécifiques soient prévues pour les entités visées ou aux droits d'accès par exemple.

Vu ce qui précède et la création d'une seule banque de données commune, à savoir la banque de données commune T.E.R., les dispositions de la loi sur la fonction de police qui sont transposées dans le présent projet visent désormais "la banque de données commune" et non plus "chaque banque de données".

Actuellement, l'article 44/2, § 2, de la loi sur la fonction de police précise que "l'article 139, alinéa 2, du Code pénal s'applique à la banque de données commune.". Ainsi, le but de cette disposition était de dire qu'une organisation dont l'objet réel est exclusivement d'ordre politique, syndical, philanthropique, philosophique ou religieux ou qui poursuit exclusivement tout autre but légitime ne peut être considérée en tant que telle comme un groupe terroriste au sens de l'article 139, paragraphe 1, du Code pénal et dès lors ne peut pas être incluse dans la base de données commune T.E.R. Par souci de clarification juridique, il est préférable de l'indiquer simplement dans la loi plutôt que par renvoi d'article.

Art. 4

Cet article transfère le principe de l'article 44/3, § 1^{er}, de la loi sur la fonction de police. Il concerne le traitement des données à caractère personnel dans la banque de données commune et précise que ce traitement doit se faire sans préjudice de la loi relative à la protection des données.

Le présent avant-projet de loi règle les questions en matière de protection des données qui sont propres aux traitements de données au sein de la banque de données commune T.E.R., à savoir quels types de données à caractère personnel y sont traitées, pour quelles finalités, pendant combien de temps, qui est responsable du traitement, quelles autorités doivent alimenter la banque de données, avec quelles catégories

immers de l'impression que er een of meer gemeenschappelijke gegevensbanken kunnen worden gecreëerd. Een veelvoud aan gemeenschappelijke gegevensbanken op het gebied van terrorisme, extremisme en het radicaliseringsproces creëren is contraproductief en gaat voorbij aan het doel om de gewenste informatie te centraliseren. Zoals hierboven toegelicht is, bestaat er in feite vanuit informatica-oogpunt bovendien slechts één gemeenschappelijke gegevensbank voor alle categorieën van personen of entiteiten die in de voornoemde koninklijke besluiten van 21 juli 2016 en 23 april 2018 worden opgesomd. Die werkelijkheid belet echter niet dat er specifieke beheersregels worden vastgesteld, bijvoorbeeld voor de beoogde entiteiten of toegangrechten.

Gelet op het voorgaande en de oprichting van een enkele gemeenschappelijke gegevensbank, met name de gemeenschappelijke gegevensbank T.E.R., beogen de bepalingen van de wet op het politieambt die door dit ontwerp worden omgezet, voortaan "de gemeenschappelijke gegevensbank" en niet langer "elke gegevensbank".

Momenteel bepaalt artikel 44/2, § 2, van de wet op het politieambt dat "artikel 139, tweede lid, van het Strafwetboek is van toepassing op de gemeenschappelijke gegevensbank.". Met deze bepaling werd dus beoogd te bepalen dat een organisatie waarvan het feitelijk oogmerk uitsluitend politiek, vakorganisatorisch, menslievend, levensbeschouwelijk of godsdienstig is of die uitsluitend enig ander rechtmatig oogmerk nastreeft, als zodanig niet beschouwd kan worden als een terroristische groep in de zin van artikel 139, eerste lid, van het Strafwetboek en dus niet in de gemeenschappelijke gegevensbank T.E.R. kan worden opgenomen. Omwille van de juridische duidelijkheid verdient het de voorkeur dit eenvoudig in de wet te vermelden in plaats van naar een artikel te verwijzen.

Art. 4

Dit artikel bevat het beginsel van artikel 44/3, § 1, van de wet op het politieambt. Het heeft betrekking op de verwerking van persoonsgegevens in de gemeenschappelijke gegevensbank en verduidelijkt dat deze verwerking onverminderd de wet gegevensbescherming moet gebeuren.

Dit wetsontwerp regelt de gegevensbeschermingskwesties die specifiek zijn voor de verwerking van gegevens in de gemeenschappelijke gegevensbank T.E.R., namelijk welke soorten persoonsgegevens daar worden verwerkt, voor welke doeleinden, hoe lang, wie verantwoordelijk is voor de verwerking, welke autoriteiten de databank moeten voeden, met welke categorieën gegevens, welke categorieën autoriteiten toegang kunnen krijgen

de données, quelles sont les catégories d'autorités qui peuvent recevoir accès ou communication de tout ou partie des données, l'obligation de journaliser les données, et quelles sont les autorités de protection des données compétentes.

Par ailleurs, dans une optique de cohérence, le législateur a choisi pour les autres règles en matière de protection des données (obligation des responsables du traitement, choix d'un sous-traitant, droits des personnes concernées, ...) de se raccrocher par analogie au titre 3, sous-titre 4 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, qui est dédié aux traitements de données à caractère personnel réalisés par l'OCAM. Bien que le contexte qui entoure les traitements de données à caractère personnel par l'OCAM au moyen de ses propres systèmes d'informations est fort différent du contexte particulier qui entoure les traitements de données à caractère personnel réalisés au sein de la banque de données commune T.E.R., nous retrouvons dans les deux cas une mutualisation de données à caractère personnel et d'informations provenant de responsables du traitement qui ne sont pas tous soumis aux mêmes obligations en matière de protection des données à caractère personnel. Il est impératif, pour garantir la plus grande sécurité juridique possible, mais également en termes de lisibilité pour les personnes concernées – et par conséquent, faciliter l'exercice de leurs droits – de définir un régime commun à ces traitements.

Suite à l'avis 73.442/2 du Conseil d'État du 7 juin 2023 et du Comité R du 13 juillet 2023 (§ 4), le nouvel alinéa relatif à la consultation des données à caractère personnel et des informations enregistrées dans la banque de données commune T.E.R. pour un traitement ultérieur à des fins historiques, scientifiques ou statistiques est supprimé en raison du double emploi de cette disposition avec l'article 162 de la loi relative à la protection des données, tel que modifié par le présent projet.

En outre, contrairement à ce qui est actuellement prévu dans la loi sur la fonction de police, la phrase “sans préjudice de la loi du 24 juin 1955 relative aux archives” a été supprimée car la référence est déjà faite à l'article 7 où elle est plus pertinente. En effet, la loi relative aux archives intervient bien au moment de l'archivage et de la suppression des données à caractère personnel et constitue même une exception au principe de suppression. Il est donc important de la mentionner mais il est plus approprié de le faire à l'article 7.

La terminologie utilisée a été adaptée aux définitions du projet.

tot of mededeling kunnen doen van alle of een deel van de gegevens, de verplichting om de gegevens vast te leggen, en welke gegevensbeschermingsautoriteiten bevoegd zijn.

Voorts heeft de wetgever met het oog op de samenhang ervoor gekozen om de andere regels inzake gegevensbescherming (verplichting van de voor de verwerking verantwoordelijken, keuze van een verwerker, rechten van de betrokkenen, ...) naar analogie te relateren aan titel 3, subtitel 4, van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, die gewijd is aan de verwerking van persoonsgegevens door het OCAD. Hoewel de context rond de verwerkingen van persoonsgegevens door het OCAD door middel van de eigen informatiesystemen ervan sterk verschilt van de specifieke context rond de verwerkingen van persoonsgegevens in de gemeenschappelijke gegevensbank T.E.R., vinden we in beide gevallen een mutualisering terug van persoonsgegevens en informatie afkomstig van verwerkingsverantwoordelijken die niet allemaal onderworpen zijn aan dezelfde verplichtingen inzake bescherming van persoonsgegevens. Om een zo groot mogelijke rechtszekerheid te waarborgen maar ook op het stuk van leesbaarheid voor de betrokken personen – en bijgevolg om de uitoefening van hun rechten te vergemakkelijken, moet een gemeenschappelijke regeling voor die verwerkingen worden bepaald.

In navolging van advies nr. 73.442/2 van 7 juni 2023 van de Raad van State en het advies van 13 juli 2023 van het Comité I (§ 4) werd een nieuw lid met betrekking tot de raadpleging van persoonsgegevens en informatie geregistreerd in de gemeenschappelijke gegevensbank T.E.R. voor een verdere verwerking van de gegevens voor historische, wetenschappelijke of statistische doeleinden geschrapt, wegens het dubbele gebruik van die bepaling met het artikel 162 van de wet tot bescherming van de persoonlijke levenssfeer, zoals gewijzigd bij dit ontwerp.

Bovendien, in tegenstelling tot wat nu in de wet op het politieambt is bepaald, is de zin “zonder afbreuk te doen aan de wet van 24 juni 1955 betreffende de archieven” geschrapt omdat die verwijzing al in artikel 7 staat, waar ze relevanter is. De archiefwet heeft immers betrekking op de archivering en de uitwissing van persoonsgegevens en vormt zelfs een uitzondering op het beginsel van de verwijdering. Het is dus belangrijk deze wet te vermelden maar het is gepaster om dat in artikel 7 te doen.

De gebruikte terminologie is aangepast aan de definities van het ontwerp.

Dans son avis n° 97/2023 du 16 juin 2023, l'Autorité de protection des données estime qu'il convient de mentionner que des statistiques seront réalisées aux fins de la publication d'un rapport d'évaluation (§§ 59 et 81). Toutefois, les autorités de contrôle de la banque de données commune T.E.R. sont le COC et le Comité R. Il leur appartient par conséquent de vérifier l'efficacité des moyens de traitements mis en œuvre et des autorités impliquées par rapport aux finalités pour lesquelles les données ont été enregistrées dans la banque de données commune T.E.R.

Section 2

Responsables du traitement et finalités

Art. 5

Cet article reprend le principe contenu dans l'article 44/11/3bis, §§ 1^{er} et 2, de la loi sur la fonction de police d'une part, et celui de l'article 2 de l'arrêté royal "TF" et de l'arrêté royal "PH", d'autre part.

Il s'agit de désigner les responsables du traitement de la banque de données commune, à savoir, les ministres de l'Intérieur et de la Justice, comme prévu actuellement, qui assument conjointement la responsabilité, mais aussi de déterminer les finalités du traitement.

Au sujet du responsable du traitement, l'Autorité de protection des données se demande vis-à-vis de quels services la banque de données est "commune" (§ 108). À cet égard, il faut préciser qu'elle est bien commune aux services de base et aux services partenaires mais pas aux services participant sur invitation aux TFL. Au sujet des préposés des responsables des traitements évoqué par l'APD (§ 108), il ne peut être question ici de la notion de préposé dans la mesure où la loi prévoit un "démembrement" des obligations du responsable du traitement (qui ne peut pas tout gérer à son niveau) qui sont partagées avec le responsable opérationnel et le gestionnaire. Chacun de ces acteurs n'a pas en effet une responsabilité concurrente mais un tâche propre concernant le traitement des données à caractère personnel. Ainsi, la loi détermine clairement le rôle et les missions de chacun de ces acteurs (responsable du traitement, responsable opérationnel et gestionnaire).

Deux finalités sont celles qui sont visées à l'article 44/11/3bis, § 2, de la loi sur la fonction de police et n'ont pas été modifiées:

In advies nr. 97/2023 van 16 juni 2023 is de Gegevensbeschermingsautoriteit van mening dat het passend is te vermelden dat er statistieken zullen worden opgesteld met het oog op de publicatie van een evaluatieverslag (§§ 59 en 81). De toezichthoudende overheden van de gemeenschappelijke gegevensbank T.E.R. zijn evenwel het COC en Comité I. Zij staan derhalve in voor de controle van de doeltreffendheid van de toegepaste verwerkingsmethoden en de autoriteiten die betrokken zijn ten opzichte van de doeleinden waarvoor de gegevens in de gemeenschappelijke gegevensbank T.E.R. werden geregistreerd.

Afdeling 2

Verwerkingsverantwoordelijken en doeleinden

Art. 5

Dit artikel herneemt het principe van artikel 44/11/3bis, §§ 1 en 2, van de wet op het politieambt enerzijds en dat van artikel 2 van het koninklijk besluit "TF" en van het koninklijk besluit "HP" anderzijds.

Het betreft de aanwijzing van de verantwoordelijken voor de verwerking van de gemeenschappelijke gegevensbank, met name de minister van Binnenlandse Zaken en de minister van Justitie, zoals nu bepaald is, die samen de verantwoordelijkheid dragen, maar ook de vaststelling van de doeleinden van de verwerking.

Wat de verwerkingsverantwoordelijke betreft, vraagt de Gegevensbeschermingsautoriteit zich af voor welke diensten de gegevensbank "gemeenschappelijk" is (§ 108). In dat verband moet worden verduidelijkt dat ze wel degelijk gemeenschappelijk is voor de basisdiensten en de partnerdiensten, maar niet voor de diensten die op uitnodiging deelnemen aan de LTF. Wat betreft de aangestelde van de verwerkingsverantwoordelijken die door de GBA worden aangehaald (§ 108), kan hier geen sprake zijn van het begrip "aangestelde", aangezien de wet voorziet in een "verdeling" van de verplichtingen van de verwerkingsverantwoordelijke (die op zijn niveau niet alles kan beheeren), die worden gedeeld met de operationeel verantwoordelijke en de beheerder. Die actoren hebben namelijk geen gedeelde verantwoordelijkheid, maar elk een eigen taak met betrekking tot de verwerking van persoonsgegevens. De wet bepaalt aldus duidelijk de rol en de opdrachten van elk van die actoren (verwerkingsverantwoordelijke, operationeel verantwoordelijke en beheerder).

Twee doeleinden zijn degene die worden bedoeld in artikel 44/11/3bis, § 2, van de wet op het politieambt en zijn niet gewijzigd:

— la nécessité stratégique, tactique ou opérationnelle de traiter en commun des données à caractère personnel et des informations pour exercer les missions respectives des services de base et des services partenaires;

— l'aide à la prise de décisions par les autorités administratives, de police administrative ou de police judiciaire. Il s'agit notamment de décisions prises afin de prévenir une menace ou un danger immédiat et sérieux pour la sécurité publique.

Au sujet de la nécessité stratégique, tactique ou opérationnelle, l'Autorité de protection des données demande de les distinguer les unes des autres et de les décrire dans la loi (avis n° 97/2023 du 16 juin 2023, § 30). Cependant, ces finalités sont liées les unes aux autres. Elles s'enrichissent l'une l'autre et s'influencent également. Les travaux parlementaires de la loi du 27 avril 2016 relatif à des mesures complémentaires en matière de lutte contre le terrorisme (DOC 54 1727/001 et suivants) permettent d'illustrer ces différentes nécessités.

Ainsi, "au niveau stratégique, il faudra par exemple, sur la base des données à caractère personnel et informations disponibles dans la banque de données commune, décider de la politique à mener dans la lutte contre ces phénomènes" (DOC 54 1727/001, p. 20). Cela se fera notamment dans le cadre du Conseil national de sécurité ou du Comité de coordination du renseignement et de la sécurité.

"Au niveau tactique, il sera question sur la base des données à caractère personnel et informations disponibles d'évaluer la façon dont les différents services vont mettre en œuvre les différentes actions à mener." (DOC 54 1727/001, p. 20). Il s'agit par exemple des actions de la TFL ou de la National task force qui coordonne la stratégie T.E.R.

"Au niveau opérationnel, il s'agira de déterminer quelles actions doivent être prises conjointement ou par chaque service particulier sur la base des données à caractère personnel et des informations disponibles ainsi que les éventuelles mesures à prendre à l'égard de certaines personnes (arrestation, auditions, ...).[...]" (DOC 54 1727/001, p. 20).

Les deux finalités précitées sont désormais complétées par la finalité de l'article 2 de l'arrêté royal "TF" et l'arrêté royal "PH", à savoir, l'analyse, l'évaluation et le suivi, en ce compris la prise de mesures, des entités validées enregistrées dans la banque de données commune T.E.R., l'analyse, l'évaluation et le suivi des entités en pré-enquêtes enregistrées dans la banque de données commune T.E.R. et l'analyse, l'évaluation et le suivi du

— de la strategische, tactische of operationele noodzaak om gezamenlijk persoonsgegevens en informatie te verwerken voor het uitoefenen van de respectievelijke bevoegdheden van de basisdiensten en de partnerdiensten;

— de hulp bij het nemen van beslissingen door de bestuurlijke overheden of de overheden van bestuurlijke politie of van gerechtelijke politie. Het betreft inzonderheid beslissingen ter voorkoming van een dreiging of een onmiddellijk en ernstig gevaar voor de openbare veiligheid.

Wat de strategische, tactische of operationele noodzaak betreft, vraagt de Gegevensbeschermingsautoriteit om ze van elkaar te onderscheiden en ze te beschrijven in de wet (advies nr. 97/2023 van 16 juni 2023, § 30). Die doeleinden zijn echter met elkaar verbonden. Ze verrijken elkaar en tevens beïnvloeden ze elkaar. Die verschillende noodzaken kunnen worden geïllustreerd aan de hand van de parlementaire werkzaamheden van de wet van 27 april 2016 inzake aanvullende maatregelen ter bestrijding van terrorisme (DOC 54 1727/001 en verdere).

Zo zal men "[o]p strategisch vlak [...] bijvoorbeeld, op basis van de persoonsgegevens en informatie die beschikbaar zijn in de gemeenschappelijke gegevensbank, moeten beslissen over het te voeren beleid in de strijd tegen deze fenomenen." (DOC 54 1727/001, blz. 20). Dat zal inzonderheid gebeuren in het kader van de Nationale Veiligheidsraad of het Coördinatiecomité voor Inlichting en Veiligheid.

"Op tactisch vlak, gaat het [erom], op basis van de beschikbare persoonsgegevens en informatie, te beoordelen op welke manier de verschillende diensten de verscheiden[e] te voeren acties zullen uitvoeren." (DOC 54 1727/001, blz. 20). Het gaat bijvoorbeeld om de acties van de LTF of de National Task Force die de T.E.R.-strategie coördineert.

"Op operationeel vlak zal het [erop aankomen] op basis van de beschikbare persoonsgegevens en informatie evenals op basis van de eventuele maatregelen die ten opzichte van bepaalde personen te nemen zijn (aanhoudingen, verhoren, ...), te bepalen welke acties gezamenlijk of door elke dienst afzonderlijk ondernomen dienen te worden. [...]" (DOC 54 1727/001, blz. 20).

De twee voornoemde doeleinden zijn nu aangevuld met het doeleinde van artikel 2 van het koninklijk besluit "TF" en het koninklijk besluit "HP", met name de analyse, de evaluatie en de opvolging, waaronder het nemen van maatregelen, van de gevalideerde entiteiten die in de gemeenschappelijke gegevensbank T.E.R. zijn geregistreerd, de analyse, de evaluatie en de opvolging van de in de gemeenschappelijke gegevensbank T.E.R.

phénomène du terrorisme et de l'extrémisme lorsqu'il peut mener au terrorisme. La banque de données commune T.E.R contribue à l'analyse, l'évaluation et au suivi des entités et du phénomène. L'exploitation des données et informations enregistrées dans cette banque de données permettra d'établir une fiche de renseignements évolutive, mise à jour en permanence par les services impliqués. Cette fiche servira à analyser et évaluer l'entité concernée. Un suivi approprié à la menace et individualisé pour cette entité pourra par conséquent être mis en œuvre par un ensemble de mesures concrètes de sécurité, de prévention et d'accompagnement spécifiques. Par rapport à l'article 2 de l'arrêté royal "TF" et l'arrêté royal "PH", les mots "sur base d'une évaluation de la menace" sont supprimés car l'interconnexion visée à l'article 9 du présent projet doit répondre à l'une des finalités fixées ici. Si le suivi du phénomène est limité à l'existence d'une évaluation de la menace par l'OCAM, l'interconnexion pour les services de base posera problème après l'archivage d'une entité.

Enfin, une nouvelle finalité est également ajoutée: la concertation coordonnée entre les services de base et les services partenaires. Cette finalité est liée à la mise en place de la plateforme de concertation visée à l'article 31. La banque de données commune T.E.R. constitue un outil au service de cette plateforme.

Suite aux préoccupations soulevées par le Délégué aux droits de l'enfant et le Commissaire aux droits de l'enfant, ainsi que l'Autorité de protection des données (avis n° 97/2023 du 16 juin 2023, § 105), une nouvelle finalité est ajoutée à la banque de données commune T.E.R. Il s'agit de l'aide à la protection, à l'accompagnement et au suivi des entités reprises dans la banque de données commune avec une attention particulière pour les mineurs. Dans ce cas précis, cela porte sur:

a) les mineurs de douze ans et plus qui sont considérés comme *foreign terrorist fighters*, *homegrown terrorist fighters*, extrémistes potentiellement violents, personnes condamnées pour terrorisme ou propagandistes de haine;

b) les enfants mineurs d'un *foreign terrorist fighters* qui répond aux critères visés à l'article 2, 7°, a) ou c), et qui ne sont pas ou ne peuvent pas être considérés comme *foreign terrorist fighters*, *homegrown terrorist fighters*, extrémistes potentiellement violents, personnes condamnées pour terrorisme ou propagandistes de haine.

geregistreerde entiteiten in vooronderzoek en de analyse, de evaluatie en de opvolging van het fenomeen van terrorisme en van extremisme wanneer het kan leiden tot terrorisme. De gemeenschappelijke gegevensbank T.E.R. draagt bij tot de analyse, de evaluatie en de opvolging van de entiteiten en het fenomeen. De exploitatie van de in deze gegevensbank geregistreerde gegevens en informatie zal het mogelijk maken een evolutieve inlichtingenfiche op te stellen die voortdurend bijgewerkt wordt door de betrokken diensten. Deze fiche zal dienen voor het analyseren en het evalueren van de betrokken entiteit. Een aan de dreiging aangepaste en aan de entiteit geïndividualiseerde opvolging zal bijgevolg uitgevoerd kunnen worden door een geheel van concrete veiligheids- en preventiemaatregelen en specifieke begeleidingsmaatregelen. Ten opzichte van artikel 2 van het koninklijk besluit "TF" en het koninklijk besluit "HP" zijn de woorden "op basis van een evaluatie van de dreiging" geschrapt, omdat de in artikel 9 van dit ontwerp bedoelde koppeling moet beantwoorden aan een van de doeleinden die hier worden vastgelegd. Indien de opvolging van het fenomeen beperkt is tot het bestaan van een evaluatie van de dreiging door het OCAD, zal de koppeling voor de basisdiensten problemen opleveren na de archivering van een entiteit.

Ten slotte, wordt ook een nieuw doeleinde toegevoegd: het gecoördineerde overleg tussen de basisdiensten en de partnerdiensten. Dit doeleinde houdt verband met de oprichting van het overlegplatform bedoeld in artikel 31. De gemeenschappelijke gegevensbank T.E.R. is een instrument ten dienste van dat platform.

Ingevolge de bekommernissen die werden geuit door de *délégué aux droits de l'enfant* en de kinderrechtencommissaris, alsook door de Gegevensbeschermingsautoriteit (advies nr. 97/2023 van 16 juni 2023, § 105), is een nieuw doeleinde toegevoegd aan de gemeenschappelijke gegevensbank T.E.R. Het betreft de hulp bij de bescherming, de begeleiding en de opvolging van de entiteiten die in de gemeenschappelijke gegevensbank zijn opgenomen, met bijzondere aandacht voor minderjarigen. In dit specifieke geval gaat het om:

a) minderjarigen van twaalf jaar en ouder die worden beschouwd als *foreign terrorist fighters*, *homegrown terrorist fighters*, potentieel gewelddadige extremisten, terrorismeveroordeelden of haatpropagandisten;

b) de minderjarige kinderen van een *foreign terrorist fighter* die beantwoordt aan de criteria bedoeld in artikel 2, 7°, a) of c), die niet worden beschouwd of niet kunnen worden beschouwd als *foreign terrorist fighters*, *homegrown terrorist fighters*, potentieel gewelddadige extremisten, terrorismeveroordeelden of haatpropagandisten.

En ce qui concerne la première catégorie de mineurs (mineurs repris en tant qu'entité) : la législation belge prévoit que des mesures peuvent être prises à l'égard de mineurs suspectés d'avoir commis un fait qualifié infraction (loi du 8 avril 1965, *Vlaamse decreet jeugd-delinquentie* dd. 15/2/2019 et décret du 18/01/2018 de la Communauté française relatif à la prévention, l'aide et la protection de la jeunesse). Dans le cadre du phénomène de terrorisme et d'extrémisme, en ce compris le processus de radicalisation, des dossiers judiciaires et des suivis TFL portent sur des mineurs concernés par des infractions terroristes. Qu'il s'agisse de mineurs emmenés par leurs parents sur zone de conflit djihadiste en vue d'intégrer une organisation terroriste, ou de mineurs ayant eux-mêmes adhéré à des idéologies extrémistes, en Belgique, le fait de pouvoir agir dans cette phase de vie où un système protectionnel existe est important pour intervenir le plus tôt possible. Et compte tenu de ce suivi multidisciplinaire, les mesures les plus appropriées pourront être prises dans l'intérêt du jeune et de la société.

Certainement dans le cadre des mineurs qui ont été emmenés par un ou ses parent(s) alors qu'ils avaient moins de 12 ans, il est important de pouvoir les considérer comme entité à partir de 12 ans – au même titre que les autres catégories – pour déterminer leur évolution idéologique sur zone et aux contacts de personnes extrémistes. Les groupements terroristes utilisent aussi des mineurs et parce qu'ils ont grandi et évolué dans cet environnement, on ne peut pas exclure qu'ils peuvent représenter un danger. Le suivi à part entière – c'est-à-dire repris comme entité de la banque de données commune T.E.R. – est donc primordial par principe de précaution que ce soit pour le mineur ou la société.

Et s'ils devaient revenir en Belgique, cette prise en considération dans la banque de données commune T.E.R. et son évaluation de la menace (qui prend en compte les informations à charge et à décharge liées à l'idéologiques, les intentions, le contexte social, les éventuelles formations ou actions menées sur zones, la problématique psychique) permettront de prendre les mesures adéquates pour accompagner ces mineurs dans le meilleur environnement possible compte tenu de sa situation spécifique.

Le législateur souhaite par ailleurs rappeler que l'approche préventive en vue de prévenir la délinquance de

Wat de eerste categorie van minderjarigen betreft (minderjarigen die zijn opgenomen als entiteit), bepaalt de Belgische wetgeving dat er maatregelen kunnen worden genomen ten aanzien van minderjarigen die ervan worden verdacht een als misdrijf omschreven feit te hebben gepleegd (wet van 8 april 1965, decreet van 15 februari 2019 van de Vlaamse overheid betreffende het jeugddelinquentierecht en decreet van 18 januari 2018 van de Franse Gemeenschap houdende het wetboek van preventie, hulpverlening aan de jeugd en jeugdbescherming). In het kader van de fenomenen terrorisme en extremisme, met inbegrip van het radicaliseringsproces, bestaan er gerechtelijke dossiers en opvolging door de LTF die betrekking hebben op minderjarigen die betrokken zijn bij terroristische misdrijven. Ongeacht het gaat om minderjarigen die door hun ouders zijn meegenomen naar een jihadistisch conflictgebied met het oog op de toetreding tot een terroristische organisatie of om minderjarigen die zelf extremistische ideologieën aanhangen in België, is het belangrijk om in die levensfase waarin er een beschermingssysteem bestaat te kunnen optreden om zo snel mogelijk te kunnen tussenkomen. Gelet op die multidisciplinaire opvolging kunnen de meest passende maatregelen worden genomen in het belang van de jongere en de samenleving.

Zeker in het kader van minderjarigen die door (een van) hun ouders zijn meegenomen terwijl ze jonger waren dan twaalf jaar is het belangrijk dat ze vanaf 12 jaar als entiteit kunnen worden beschouwd – net als de andere categorieën – om hun ideologische evolutie in het gebied en ingevolge hun contacten met extremistische personen in kaart te brengen. Terroristische groeperingen gebruiken ook minderjarigen en omdat ze zijn opgegroeid en zich hebben ontwikkeld in die omgeving kan niet worden uitgesloten dat ze een gevaar vormen. De volwaardige opvolging – dat wil zeggen als entiteit opgenomen in de gemeenschappelijke gegevensbank T.E.R. – is dus uit voorzorg cruciaal, zowel voor de minderjarige als voor de samenleving.

Indien ze zouden terugkeren naar België, kunnen, doordat ze in aanmerking zijn genomen in de gemeenschappelijke gegevensbank T.E.R. en op basis van de dreigingsevaluatie (waarbij rekening wordt gehouden met de informatie à charge en à décharge in verband met de ideologie, de intenties, de maatschappelijke context, de eventuele opleidingen of ondernomen acties in het gebied en de psychische problematiek), passende maatregelen worden genomen om die minderjarigen te begeleiden in de best mogelijke omgeving rekening houdend met hun specifieke situatie.

De wetgever wenst ook te herhalen dat de preventieve aanpak ter voorkoming van delinquentie van deze

cette catégorie de mineurs reste la voie à privilégier. Pour ces mineurs et dans cet objectif particulier, les CSIL-R doivent bien entendu jouer leur rôle dans une logique sociale inclusive.

En ce qui concerne la seconde catégories de mineurs: seront concernés ici, les données relatives au nom, prénom, date de naissance et genre des enfants mineurs, biologiques ou adoptés d'un parent, personne physique qui est enregistré dans la banque de données commune T.E.R. comme *foreign terrorist fighter* qui séjourne ou a séjourné en zone de conflit djihadiste. Il ne s'agit ni de les reprendre dans la banque de données commune T.E.R. comme "entités" en tant que telles (ils ne sont donc pas repris à titre principal) ni d'enregistrer les enfants de toutes les entités enregistrées mais uniquement ceux qui séjournent ou ont séjournés en zone de conflit djihadiste. Ceci pour pouvoir mettre en place les mesures de protection et de suivi les plus appropriées en cas de retour.

L'objectif est d'une part de pouvoir avoir un aperçu le plus précis possible des enfants qui sont sur zones de combat djihadiste. En effet, la plupart de ces enfants sont nés sur zone et ne sont pas repris dans le registre national. Il est donc important de pouvoir disposer d'informations quant à leur existence et le lien avec un parent repris dans la banque de données commune T.E.R. comme entité ayant rejoint une organisation terroriste sur une zone de combat djihadiste.

Et, d'autre part, lors de leur retour, il est nécessaire de disposer des informations quant au lien qui existe avec un adulte dans le cadre du suivi socio-préventif de ses enfants. Par exemple, un fois de retour de zone de combat djihadiste avec leur mère, lorsque celle-ci ira en prison, l'enfant sera pris en charge par des instances de protection de la jeunesse dans le cadre de sa protection et les mesures quant au suivi de sa santé, de son environnement de vie devront être prises. Et lors de la sortie de prison de la mère, il est important d'assurer un lien quant à l'évolution de la mère et de l'enfant. Ceci se fait en CSIL-R, plateforme socio-préventive créée par la loi du 30 juillet 2018. Mais ici aussi, il est important de savoir que la mère a des enfants pour mettre en place les mesures et actions de réintégration respective.

Par ailleurs, les enfants de cette deuxième catégorie n'apparaissent pas dans la banque de données commune T.E.R. si leur nom est introduit. Comme explicité ci-avant, ils ne sont pas soumis au même suivi qu'une

categorie van minderjarigen de voorkeur blijft genieten. Voor deze minderjarigen en voor dit specifieke doel, moeten de LIVC-R natuurlijk hun rol spelen in een inclusieve sociale aanpak.

Voor de tweede categorie van minderjarigen gaat het om de gegevens met betrekking tot de naam, de voornaam, de geboortedatum en het geslacht van de biologische of geadopteerde minderjarige kinderen van een ouder, die een natuurlijke persoon is die in de gemeenschappelijke gegevensbank T.E.R. is opgenomen als *foreign terrorist fighter* die in een jihadistisch conflictgebied verblijft of heeft verbleven. Het is niet de bedoeling om ze in de gemeenschappelijke gegevensbank T.E.R. op te nemen als "entiteiten" als dusdanig (in de hoedanigheid van "hoofdentiteit" dus), en ook niet om de kinderen van alle opgenomen entiteiten erin op te nemen, maar louter om diegenen die in een jihadistisch conflictgebied verblijven of hebben verbleven erin op te nemen. Doel daarvan is om de geschikteste beschermings- en opvolgingsmaatregelen te kunnen nemen in geval van terugkeer.

Het is ten eerste de bedoeling om een zo nauwkeurig mogelijk overzicht te kunnen hebben van de kinderen die in een jihadistisch strijdgebied verkeren. De meeste van die kinderen zijn namelijk in dat gebied geboren en zijn niet opgenomen in het Rijksregister. Het is dus van belang om te kunnen beschikken over informatie met betrekking tot hun bestaan en de band met een ouder die in de gemeenschappelijke gegevensbank T.E.R. is opgenomen als entiteit die zich heeft aangesloten bij een terroristische organisatie in een jihadistisch strijdgebied.

Ten tweede is het nodig om bij hun terugkeer over informatie te beschikken over de bestaande band met een volwassene in het kader van de sociopreventieve opvolging van diens kinderen. Zodra het kind bijvoorbeeld met zijn moeder is teruggekeerd uit een jihadistisch strijdgebied, zal het, wanneer de moeder naar de gevangenis moet, worden opgevangen door jeugdbeschermingsinstanties in het kader van zijn bescherming en moeten er maatregelen ter opvolging van zijn gezondheid en zijn leefomgeving worden genomen. Wanneer de moeder vrijkomt uit de gevangenis, is het op het vlak van de evolutie van de moeder en het kind belangrijk om voor een band te zorgen. Dat gebeurt in de LIVC R, een sociopreventief platform dat werd opgericht bij de wet van 30 juli 2018. Ook hier is het echter van belang te weten dat de moeder kinderen heeft om de respectievelijke maatregelen en re-integratieacties door te voeren.

De kinderen van die tweede categorie verschijnen overigens niet in de gemeenschappelijke gegevensbank T.E.R. wanneer hun naam wordt ingevoerd. Zoals hierboven uitgelegd, zijn ze niet onderworpen aan dezelfde

entité enregistrée en tant que telle. Ils sont également considérés comme des enfants en danger.

Ce n'est donc que dans les deux cas spécifiques précités (enfant d'un FTF catégorie 1 ou catégorie 3) qu'un enfant est traité dans les données relatives à son parent, pour une finalité de protection, de suivi et de réintégration.

Enfin, comme le rappellent les délégués aux droits de l'enfant, il y a lieu de tenir compte de l'article 40 de la Convention internationale relative aux droits de l'enfant dans le cadre du traitement à réserver aux enfants qu'ils soient âgés de plus de 12 ans ou de moins de 12 ans. Cet article 40 prévoit que: "Les États parties reconnaissent à tout enfant suspecté, accusé ou convaincu d'infraction à la loi pénale le droit à un traitement qui soit de nature à favoriser son sens de la dignité et de la valeur personnelle, qui renforce son respect pour les droits de l'homme et les libertés fondamentales d'autrui, et qui tienne compte de son âge ainsi que de la nécessité de faciliter sa réintégration dans la société et de lui faire assumer un rôle constructif au sein de celle-ci."

À noter que le paragraphe 3 de l'article 44/11/3bis de la loi sur la fonction de police n'est pas repris dans le présent projet. En effet, selon ce paragraphe 3, "Préalablement à sa création, les ministres de l'Intérieur et de la Justice déclarent la banque de données commune, ainsi que les modalités de traitement, dont celles relatives à l'enregistrement des données, et les différentes catégories et types de données à caractère personnel et d'informations traitées, aux Comité et l'Organe de contrôle visés à l'article 44/11/3quinquies/2, qui émettent conjointement un avis dans les 30 jours à partir de la réception de la déclaration.". Dans la mesure où la banque de données commune, les modalités de traitement et les différentes catégories et types de données à caractère personnel et d'informations traitées sont directement créés par la loi, avec les garanties qui s'y attachent, ce paragraphe n'a plus lieu d'être.

opvolging als een entiteit die als dusdanig is opgenomen. Ze worden eveneens beschouwd als kinderen die in gevaar verkeren.

De gegevens van een kind worden dus enkel in de twee voornoemde specifieke gevallen (kind van een FTF categorie 1 of categorie 3) verwerkt in de gegevens betreffende zijn ouder, met het oog op bescherming, opvolging en re-integratie.

Tot slot, zoals de afgevaardigden voor de rechten van het kind hebben aangegeven, moet artikel 40 van het Internationaal Verdrag inzake de Rechten van het Kind in aanmerking worden genomen bij de behandeling van kinderen, ongeacht of ze ouder dan of jonger dan 12 jaar zijn. Dit artikel 40 staat dat: "De Staten die partij zijn, erkennen het recht van ieder kind dat wordt verdacht van, vervolgd wegens of veroordeeld terzake van het begaan van een strafbaar feit, op een wijze van behandeling die geen afbreuk doet aan het gevoel van waardigheid en eigenwaarde van het kind, die de eerbied van het kind voor de rechten van de mens en de fundamentele vrijheden van anderen vergroot, en waarbij rekening wordt gehouden met de leeftijd van het kind en met de wenselijkheid van het bevorderen van de herintegratie van het kind en van de aanvaarding door het kind van een opbouwende rol in de samenleving."

Er moet worden opgemerkt dat artikel 44/11/3bis, § 3, van de wet op het politieambt niet wordt hernomen in dit ontwerp. In die paragraaf 3 is immers het volgende gesteld: "Voorafgaand aan haar oprichting, doen de ministers van Binnenlandse Zaken en van Justitie aangifte van de gemeenschappelijke gegevensbank alsook van de verwerkingsmodaliteiten, waaronder deze met betrekking tot de registratie van de gegevens en van de verschillende categorieën en types van persoonsgegevens en informatie die verwerkt worden bij het Comité en het Controleorgaan bedoeld in artikel 44/11/3quinquies/2, die gezamenlijk een advies uitbrengen binnen de 30 dagen vanaf de ontvangst van de aangifte.". Die paragraaf heeft geen bestaansreden meer aangezien de gemeenschappelijke gegevensbank, de verwerkingsmodaliteiten en de verschillende categorieën en types van persoonsgegevens en informatie die verwerkt worden, rechtstreeks worden voorzien in de wet, met de bijhorende waarborgen.

Section 3

Traitement des données à caractère personnel

Art. 6

L'article 6 est relatif aux traitements des données à caractère personnel qui figurent dans la banque de données commune. Il reprend l'actuel article 44/11/3*bis*, § 4, de la loi sur la fonction de police ainsi que l'article 6 de l'arrêté royal "TF" et de l'arrêté royal "PH".

Dans son avis n° 97/2023 du 16 juin 2023, l'Autorité de protection des données relève plusieurs points à cet égard:

— les finalités des traitements de données à caractère personnel par les services de bases et les services partenaires doivent être déterminées (§ 31.) Le comité R a fait la même remarque dans son avis du 13 juillet 2023 (§ 2). Or, la banque de données commune est créée en raison des traitements existants. C'est le principe même d'une banque de données commune d'avoir des traitements. Les finalités des traitements par les différents services sont donc celles de la banque de données commune T.E.R.;

— pour chacun des services disposant d'un droit d'écriture, il convient de démontrer en quoi la finalité de chacun des traitements ultérieurs des données visées dans l'article 6 est compatible avec la finalité pour laquelle elles ont été collectées (§ 32). Sur ce point, il est renvoyé au commentaire de l'article 30 relatif à la responsabilité de la qualité des données à caractère personnel et des informations enregistrées dans la banque de données commune T.E.R. Les principes du traitement des données à caractère personnel doivent être respectés par chaque service partenaire sur base de sa propre législation. En outre, les responsables du traitement doivent tenir un registre des traitements de données qu'ils effectuent;

— l'enregistrement dans la banque de données commune ne peut aboutir à ce qu'un service traite des données à caractère personnel qu'il ne serait pas autorisé à traiter en vertu de ses finalités propres (§ 34). En réalité, il en est déjà tenu compte. La distinction se fait au niveau des droits d'accès. Au niveau technique, il faut s'assurer que la banque de données soit consultable de façon proportionnelle. Les développements de la banque de données prennent en compte cela, raison pour laquelle il existe des droits d'accès différents selon le partenaire. À titre d'exemple, on peut citer les Maisons de justice qui ont un accès uniquement pour les personnes à propos desquelles elles ont reçu un mandat. Cependant, si un

Afdeling 3

Verwerking van persoonsgegevens

Art. 6

Artikel 6 heeft betrekking op de verwerkingen van persoonsgegevens die zijn opgenomen in de gemeenschappelijke gegevensbank. Het herneemt het huidige artikel 44/11/3*bis*, § 4, van de wet op het politieambt alsmede artikel 6 van het koninklijk besluit "TF" en van het koninklijk besluit "HP".

In advies nr. 97/2023 van 16 juni 2023 haalt de Gegevensbeschermingsautoriteit verschillende punten aan in dat verband:

— de doeleinden van de verwerking van persoonsgegevens door de basisdiensten en de partnerdiensten moeten worden vastgesteld (§ 31). Comité I heeft dezelfde opmerking geformuleerd in het advies van 13 juli 2023 (§ 2). De gemeenschappelijke gegevensbank is echter opgericht met het oog op de bestaande verwerkingen. Het principe van een gemeenschappelijke gegevensbank bestaat erin dat er sprake is van verwerkingen. De doeleinden van de verwerking door de verschillende diensten zijn dus die van de gemeenschappelijke gegevensbank T.E.R.;

— voor elke dienst met een schrijfrecht moet worden aangetoond hoe het doel van elke verdere verwerking van de in artikel 6 bedoelde gegevens verenigbaar is met het doel waarvoor ze zijn verzameld (§ 32). In dat verband wordt verwezen naar de toelichting bij artikel 30 betreffende de verantwoordelijkheid voor de kwaliteit van de persoonsgegevens en de informatie die geregistreerd zijn in de gemeenschappelijke gegevensbank T.E.R. De beginselen inzake de verwerking van persoonsgegevens moeten door elke partnerdienst worden nageleefd op basis van zijn eigen wetgeving. Voorts moeten de verwerkingsverantwoordelijken een register bijhouden van de gegevensverwerkingen die ze uitvoeren;

— de registratie in de gemeenschappelijke gegevensbank kan er niet toe leiden dat een dienst persoonsgegevens verwerkt die hij op grond van zijn eigen doeleinden niet mag verwerken (§ 34). In feite is daarmee reeds rekening gehouden. Het onderscheid wordt gemaakt op het niveau van de toegangsrechten. Op technisch niveau moet men zich ervan vergewissen dat de gegevensbank op evenredige wijze kan worden geraadpleegd. In de ontwikkeling van de gegevensbank is daarmee rekening gehouden, daarom bestaan er verschillende toegangsrechten per partner. De justitiehuizen hebben bijvoorbeeld enkel toegang voor de personen voor wie ze een opdracht hebben gekregen. Indien een partnerdienst

service partenaire consulte la banque de données, c'est qu'elle a une raison de le faire car elle est intéressée par une personne. Et cela se fait toujours dans le cadre des finalités de la banque de données commune T.E.R. La mise en commun concerne ce qui est nécessaire pour la réalisation des finalités;

— aux §§ 35 et 36, l'Autorité de protection des données fait le lien avec les lois organiques de chaque service partenaire et leurs finalités. Il faut préciser que chaque service est tenu de respecter la loi, en particulier sa loi organique, et qu'il n'est pas question ici de créer des droits nouveaux. Ces services ont un accès à la banque de données commune T.E.R. car cela est nécessaire dans le cadre de leurs missions. Par ailleurs, ces services, dans le cadre de leurs finalités propres, peuvent avoir des informations utiles à la lutte contre le terrorisme, raison pour laquelle il y a une mise en commun de l'information. Toutefois, ils n'en deviennent pas pour autant des "agents" compétents en matière de terrorisme. En ce qui concerne le caractère proportionnel des accès/communications, il s'apprécie in casu. En conclusion, chaque service travaille dans le cadre de ses missions (art. 24, § 2) et l'objectif de la présente loi n'est pas de les modifier, raison pour laquelle, il n'est pas question de modifier les lois organiques des services partenaires;

— les finalités des accès par les services partenaires doivent être déterminées pour chaque catégorie de donnée (§ 37). Dans les faits, cela est déjà le cas dans la mesure où le service partenaire sélectionne les informations pertinentes dans le cadre de son traitement et de ses missions;

— concernant la bonne pratique visant la détermination de limites ou l'énonciation de circonstances dans lesquelles un traitement serait constitutif d'un détournement (§ 39), il faut rappeler que l'exposé des motifs vise à expliquer le projet de loi et n'a pas vocation à devenir un guide de bonnes pratiques. Il va de soi que les services travaillent dans le cadre des finalités et des missions de la loi;

— le projet n'indique pas quelles données seront traitées par quels services (§§ 93 à 95). Les catégories de données visées sont une liste de données potentiellement exploitables. Il est clair que chaque partenaire traite les données qui lui sont nécessaires dans le cadre de ses missions légales et du respect des principes de d'adéquation, de pertinence et du caractère non excessif. Chaque service ne consulte que les informations qui sont pertinentes pour lui. Pour rappel, la journalisation permet d'exercer un contrôle des traitements effectués dans la banque de données commune T.E.R. Enfin, en ce qui concerne l'adaptation des solutions

de la banque de données, il faut préciser que chaque service est tenu de respecter la loi, en particulier sa loi organique, et qu'il n'est pas question ici de créer des droits nouveaux. Ces services ont un accès à la banque de données commune T.E.R. car cela est nécessaire dans le cadre de leurs missions. Par ailleurs, ces services, dans le cadre de leurs finalités propres, peuvent avoir des informations utiles à la lutte contre le terrorisme, raison pour laquelle il y a une mise en commun de l'information. Toutefois, ils n'en deviennent pas pour autant des "agents" compétents en matière de terrorisme. En ce qui concerne le caractère proportionnel des accès/communications, il s'apprécie in casu. En conclusion, chaque service travaille dans le cadre de ses missions (art. 24, § 2) et l'objectif de la présente loi n'est pas de les modifier, raison pour laquelle, il n'est pas question de modifier les lois organiques des services partenaires;

— in de §§ 35 en 36 legt de Gegevensbeschermingsautoriteit de link met de organieke wetten van elke partnerdienst en de doeleinden ervan. Er dient te worden verduidelijkt dat elke dienst de wet moet naleven, in het bijzonder zijn organieke wet, en dat het hier niet de bedoeling is om nieuwe rechten te creëren. Die diensten hebben toegang tot de gemeenschappelijke gegevensbank T.E.R. omdat dat noodzakelijk is in het kader van hun opdrachten. Voorts kunnen die diensten in het kader van hun eigen doeleinden beschikken over nuttige informatie voor de bestrijding van terrorisme, vandaar dat de informatie wordt gebundeld. Dat maakt van hen evenwel nog geen "agenten" die bevoegd zijn op het vlak van terrorisme. Het evenredige karakter van de toegang/mededeling wordt in casu beoordeeld. Tot besluit: elke dienst werkt in het kader van zijn opdrachten (art. 24, § 2) en het is niet de bedoeling van deze wet om die te wijzigen, vandaar dat er geen sprake is van een wijziging van de organieke wetten van de partnerdiensten;

— de doeleinden van de toegang door de partnerdiensten moeten voor elke gegevenscategorie worden vastgesteld (§ 37). In de praktijk is dat reeds het geval, aangezien de partnerdienst de relevante informatie selecteert in het kader van zijn verwerking en zijn opdrachten;

— wat de goede praktijk inzake het stellen van grenzen of het vermelden van de omstandigheden waarin een verwerking onrechtmatig van het doeleinde zou afwijken (§ 39) betreft, dient erop te worden gewezen dat de memorie van toelichting tot doel heeft om het wetsontwerp te verduidelijken en niet om een gids met goede praktijken te worden. Het spreekt voor zich dat de diensten hun werk uitvoeren in het kader van de doeleinden en de opdrachten van de wet;

— in het ontwerp wordt niet vermeld welke gegevens door welke diensten zullen worden verwerkt (§§ 93 tot 95). De categorieën van gegevens die worden beoogd, vormen een lijst van potentieel exploitbare gegevens. Het is duidelijk dat elke partner de gegevens verwerkt die voor hem noodzakelijk zijn in het kader van zijn wettelijke opdrachten en de inachtneming van de principes van toereikendheid, relevantie en de niet-bovenmatige aard. Elke dienst raadpleegt enkel de informatie die voor hem ter zake dienend is. Ter herinnering: de logbestanden maken het mogelijk om de in de gemeenschappelijke gegevensbank T.E.R. uitgevoerde verwerkingen te

technologiques aux normes et non l'inverse (§ 95), on peut indiquer que la banque de données commune évolue sur le plan technique en fonction des décisions qui sont prises par les responsables du traitement et le responsable opérationnel, après une discussion au sein des comités de pilotage dédiés à la banque de données commune. Dans ce contexte, le gestionnaire reçoit aussi les précisions quant aux priorités à accorder entre les différents développements. Il n'est pas possible de les mener tous de front, ni de les mener instantanément. La méthode suivie donne néanmoins la garantie que ce sont bien les besoins et les obligations, y compris en matière de protection des personnes à l'égard des traitements de données, qui commandent les développements techniques et non l'inverse. En outre, selon le RGPD, le responsable du traitement doit s'assurer d'offrir la meilleure solution possible selon ses moyens;

— la nécessité de démontrer, sur base d'éléments factuels et objectifs, l'efficacité du traitement de données à caractère personnel envisagé pour atteindre l'objectif recherché (§ 97). Le présent projet repose sur le principe du caractère adéquat, pertinent et non excessif des catégories de données traitées dans la banque de données au regard des missions visées à l'article 3, et des finalités visées à l'article 5, alinéa 2. En outre, le législateur ne fait pas œuvre scientifique, mais démocratique. La validité du travail législatif n'est pas soumise à la production de sources documentaires ou à la vérification d'une méthode particulière, sans préjudice des exigences spécifiques que prévoient la loi elle-même ou la Constitution. Le projet ou la proposition est soumis au Parlement: ce sont ses membres qui le vérifieront et l'approuveront, l'amenderont ou le refuseront;

— au sujet du caractère exact à jour des données traitées (§ 98), il faut préciser que le projet ne prévoit pas un mécanisme structurel comme celui de l'article 646 du Code d'instruction criminelle mais une procédure est mise sur pied pour s'assurer que les données disponibles sont à jour. Ainsi chaque service est responsable de la qualité des données qu'il introduit dans la banque de données;

L'article 6, § 1^{er}, reprend l'actuel article 44/11/3bis, § 4, alinéa 1^{er}, de la loi sur la fonction de police relatif à l'objectif de la banque de données commune, à savoir le traitement de certaines catégories de données à caractère personnelle relatives aux personnes, aux groupements, aux organisations et aux phénomènes qui sont adéquates, pertinentes et non excessives au

contrôler. Wat tot slot de aanpassing van de technologische toepassingen aan de normen in plaats van omgekeerd (§ 95) betreft, kan worden gesteld dat de gemeenschappelijke gegevensbank op technisch vlak evolueert op basis van de beslissingen die worden genomen door de verwerkingsverantwoordelijken en de operationeel verantwoordelijke na een bespreking in de stuurgroepen die zich toeleggen op de gemeenschappelijke gegevensbank. In die context ontvangt de beheerder ook verduidelijkingen met betrekking tot de prioriteiten die moeten worden gesteld tussen de verschillende ontwikkelingen. Het is niet mogelijk om ze allemaal tegelijk te realiseren, noch om ze onmiddellijk te realiseren. De gevolgde methode biedt evenwel de garantie dat het wel degelijk de behoeften en verplichtingen, met inbegrip van de bescherming van personen in verband met de verwerking van gegevens, zijn die de technische ontwikkelingen aansturen, en niet omgekeerd. Voorts moet de verwerkingsverantwoordelijke, volgens de AVG, ervoor zorgen dat hij de best mogelijke oplossing overeenkomstig zijn middelen aanbiedt;

— de noodzaak om, op basis van feitelijke en objectieve elementen, aan te tonen dat de voorgestelde verwerking van persoonsgegevens doeltreffend is voor het bereiken van het beoogde doel (§ 97). Dit ontwerp berust op het beginsel van het toereikende, ter zake dienende en niet overmatige karakter van de categorieën van gegevens die in de gegevensbank worden verwerkt in verhouding tot de opdrachten bedoeld in artikel 3, en de doeleinden bedoeld in artikel 5, tweede lid. Voorts levert de wetgever geen wetenschappelijk, maar democratisch werk. De geldigheid van het wetgevend werk is niet onderworpen aan de overlegging van documentatiebronnen of aan de controle van een specifieke methode, onverminderd de specifieke vereisten waarin de wet zelf of de Grondwet voorziet. Het ontwerp of het voorstel wordt voorgelegd aan het parlement: het zijn de parlementsleden die het controleren en goedkeuren, wijzigen of weigeren;

— wat betreft het nauwkeurige en actuele karakter van de verwerkte gegevens (§ 98), moet worden verduidelijkt dat het ontwerp niet voorziet in een structureel mechanisme zoals dat in artikel 646 van het Wetboek van Strafvordering, maar dat er een procedure is opgezet om ervoor te zorgen dat de beschikbare gegevens actueel zijn. Zo is elke dienst verantwoordelijk voor de kwaliteit van de gegevens die hij in de gegevensbank invoert;

Artikel 6, § 1, herneemt het huidige artikel 44/11/3bis, § 4, eerste lid, van de wet op het politieambt met betrekking tot de doelstelling van de gemeenschappelijke gegevensbank, met name de verwerking van bepaalde categorieën van persoonsgegevens met betrekking tot personen, groeperingen, organisaties en fenomenen die toereikend, ter zake dienend en niet overmatig zijn

regard des missions visées à l'article 3, et des finalités visées à l'article 5, alinéa 2. De même, comme cela est actuellement prévu par l'article 44/3, § 1, alinéa 2, de la loi sur la fonction de police, il est précisé que les données à caractère personnel et les informations traitées dans la banque de données commune T.E.R. présentent un lien direct avec la finalité du traitement.

L'article 6, § 2, alinéa 1^{er}, détermine les types de données à caractère personnel qui sont traitées dans la banque de données commune. Comme indiqué précédemment, suite à l'avis du Comité R du 13 juillet 2023 au sujet des définitions (§ 18), le caractère non classifié des données traitées dans la banque de données commune T.E.R. est repris ici. Les catégories de données sont celles de l'article 6 de l'arrêté royal "TF" et de l'arrêté royal "PH". Elles ont toutefois été précisées. Il faut rappeler que les données enregistrées dans la banque de données commune T.E.R. pourront être utilisées pour augmenter ou au contraire pour diminuer le niveau de la menace de l'entité concernée. Illustrons ce propos. Si via la consultation des données dans la banque de données commune T.E.R., il apparaît qu'une personne physique suit des formations en vue de se réinsérer dans la société, ne fréquente plus de milieux extrémistes et ne commet plus depuis plusieurs années d'infractions en lien avec les finalités T.E.R., le niveau de la menace de cette personne sera beaucoup plus bas que si, sur la base des informations récoltées, il ressort qu'elle suit des formations pour manier des explosifs, qu'elle ne se présente pas à ses convocations avec les assistants de Justice et qu'elle tient des propos extrémistes, appelant à la haine consignés dans des procès-verbaux de la police.

I. — DONNÉES D'IDENTIFICATION

A. Entités personnes physiques

A.1. La première catégorie de données à caractère personnel traitées sont les données d'identification d'une personne physique majeure ou mineure de douze ans et plus. Cette catégorie a été détaillée. Il s'agit donc:

1) des noms, prénoms et les alias (alias, surnom, sobriquet etc.);

Lorsque des personnes physiques sont enregistrées dans la banque de données commune T.E.R., il convient de les identifier correctement et leurs nom et prénoms sont les premières données nécessaires à cette identification. Elles ne sont néanmoins pas toujours

in verhouding tot de opdrachten bedoeld in artikel 3, en de doeleinden bedoeld in artikel 5, tweede lid. Evenzo, aangezien hierin nu is voorzien bij artikel 44/3, § 1, tweede lid, van de wet op het politieambt, wordt verduidelijkt dat de persoonsgegevens en informatie die in de gemeenschappelijke gegevensbank T.E.R. worden verwerkt, in rechtstreeks verband staan met het doeleinde van de verwerking.

In artikel 6, § 2, eerste lid wordt bepaald welke types van persoonsgegevens in de gemeenschappelijke gegevensbank worden verwerkt. Zoals eerder aangegeven, is, in navolging van het advies van Comité I van 13 juli 2023 over de definities (§ 18), de niet-geclassificeerde aard van de gegevens die worden verwerkt in de gemeenschappelijke gegevensbank T.E.R. hierin opgenomen. De categorieën van gegevens zijn die van artikel 6 van het koninklijk besluit "TF" en van het koninklijk besluit "HP". Ze zijn echter wel gespecificeerd. Er moet op worden gewezen dat de gegevens in de gemeenschappelijke gegevensbank T.E.R. kunnen worden gebruikt om het dreigingsniveau van de betrokken entiteit te verhogen of juist te verlagen. Ter illustratie: indien uit de raadpleging van de gegevens in de gemeenschappelijke gegevensbank T.E.R. blijkt dat een bepaalde natuurlijke persoon opleidingen volgt om zich in de maatschappij te re-integreren, zich niet meer in extremistische kringen ophoudt en al jaren geen misdrijven meer pleegt in verband met de T.E.R.-doeleinden, zal zijn dreigingsniveau veel lager liggen dan als uit de vergaarde informatie blijkt dat hij opleidingen volgt om explosieven te hanteren, hij niet op zijn bijeenkomsten met de justitieassistenten komt opdagen en extremistische, haatzaaiende uitspraken doet die in processen-verbaal van de politie zijn vastgesteld.

I. — IDENTIFICATIEGEGEVENS

A. Entiteiten die natuurlijke personen zijn

A. 1. De eerste categorie van persoonsgegevens die worden verwerkt zijn de identificatiegegevens van een meerderjarige natuurlijke persoon of een minderjarige natuurlijke persoon van twaalf jaar en ouder. Deze categorie werd gedetailleerd. Het gaat dus om:

1) naam, voornamen en alias (alias, bijnaam, enz.);

Wanneer natuurlijke personen worden geregistreerd in de gemeenschappelijke gegevensbank T.E.R., moeten ze correct worden geïdentificeerd, waartoe hun naam en voornamen de eerste noodzakelijke gegevens zijn. Die volstaan echter niet altijd, omdat bepaalde

suffisantes car certaines personnes utilisent des alias pour dissimuler leur identité réelle et compliquer ainsi la détection de relations entre des données les concernant. L'enregistrement des alias permet de faire le lien avec des identités réelles connues. En procédant de cette manière, les recherches dans la banque de données donnent toutes les données relatives à une personne. L'enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 a pu elle-même constater que les "*foreign terrorist fighters*" utilisent plusieurs alias (Troisième rapport intermédiaire sur le volet architecture de la sécurité, point 81, p. 86). Le point 174 (p. 243) de ce même rapport précise que "L'identification des auteurs et des suspects impliqués dans les attentats de Paris et de Bruxelles n'a pas été chose aisée. En effet, les auteurs des attaques utilisaient plusieurs surnoms et fausses identités (alias) et recouraient souvent à des documents d'identité (parfois volés) professionnellement falsifiés". Pour contrer ces problèmes, il s'impose que les services de base et les services partenaires partagent dans la banque de données commune T.E.R. les noms et prénoms mais aussi les alias dont ils ont connaissance.

2) s'il échet, le numéro d'identification du Registre national des personnes physiques ou du registre des étrangers;

Avec cette même préoccupation d'identifier correctement les personnes physiques enregistrées, il doit pouvoir être recouru dès que c'est possible au numéro d'identification du Registre national ou, comme suggéré par le Conseil d'État dans son avis 73.442/2 du 7 juin 2023, du registre des étrangers. Son traitement dans la banque de données donne aux utilisateurs la garantie que l'identité a pu être confirmée par la source authentique qu'est le Registre national ou le registre des étrangers. D'autre part, le numéro d'identification repris dans la banque de données permet aux services de base et partenaires de faire le lien avec un même numéro d'identification enregistré dans leur propre banque de données. Le nom et le prénom sont nettement moins fiables dans ce contexte en raison de l'orthographe ou de règles de gestion des noms et prénoms pouvant être différentes dans les systèmes.

Il faut bien entendu que les services disposent des autorisations nécessaires pour traiter du numéro d'identification du Registre national dans leur propre système ou qu'il y ait une interconnexion entre la banque de données commune T.E.R. et le registre national, comme c'est prévu à l'article 9.

personnes aliasen gebruiken om hun werkelijke identiteit te verbergen en er aldus voor te zorgen dat er moeilijker verbanden kunnen worden gelegd tussen gegevens die op hen betrekking hebben. De registratie van aliasen maakt het mogelijk de link te leggen met bekende werkelijke identiteiten. Door op die manier te werk te gaan, leveren opzoeken in de gegevensbank alle gegevens met betrekking tot een persoon op. Het parlementair onderzoek belast met het onderzoek naar de omstandigheden die hebben geleid tot de terroristische aanslagen van 22 maart 2016 kon zelf vaststellen dat "*foreign terrorist fighters*" meerdere aliasen gebruiken (Derde tussentijds verslag over het onderdeel "Veiligheidsarchitectuur", punt 81, blz. 86). In punt 174 (blz. 243) van hetzelfde verslag wordt het volgende verduidelijkt: "Het identificeren van de verdachten en de daders die betrokken waren bij de aanslagen in Parijs en in Brussel is niet van een leien dakje gelopen. Het is namelijk zo dat de daders van de aanslagen meerdere roepnamen en valse identiteiten (aliasen) gebruikten. Dikwijls werd hierbij gebruik gemaakt van professioneel vervalste (soms gestolen) identiteitsdocumenten." Om die problemen tegen te gaan, moeten de basisdiensten en de partnerdiensten de namen en voornamen, maar eveneens de aliasen waarvan ze kennis hebben, delen in de gemeenschappelijke gegevensbank T.E.R.

2) indien van toepassing, het identificatienummer van het Rijksregister van de natuurlijke personen of van het vreemdelingenregister;

Vanuit dezelfde bekommernis om de geregistreerde natuurlijke personen correct te identificeren, moet zodra dat mogelijk is een beroep kunnen worden gedaan op het identificatienummer van het Rijksregister of, zoals gesuggereerd door de Raad van State in advies nr. 73.442/2 van 7 juni 2023, van het vreemdelingenregister. De verwerking ervan in de gegevensbank biedt de gebruikers de garantie dat de identiteit kon worden bevestigd door het Rijksregister of het vreemdelingenregister als authentieke bron. Daarnaast stelt het in de gegevensbank vermelde identificatienummer de basis- en partnerdiensten in staat de link te leggen met eenzelfde identificatienummer dat in hun eigen gegevensbank is geregistreerd. De naam en voornaam zijn in die context veel minder betrouwbaar vanwege de spelling of regels voor het beheer van de namen en voornamen die kunnen verschillen in de systemen.

De diensten moeten uiteraard beschikken over de nodige machtigingen voor de verwerking van het identificatienummer van het Rijksregister in hun eigen systeem of er moet een koppeling zijn tussen de gemeenschappelijke gegevensbank T.E.R. en het Rijksregister, zoals is bepaald in artikel 9.

3) l'adresse;

L'adresse permet de localiser la personne lorsqu'il est nécessaire de rentrer en contact avec elle. Ce n'est pas le seul but de cette donnée. En effet, l'adresse qui provient du Registre national détermine aussi la "Task force locale" compétente ainsi que les autorités et les services qui devront intervenir dans le cadre d'actes de prévention ou de suivi de la personne.

4) le sexe et/ou genre;

Le sexe et/ou le genre est une donnée qui caractérise les personnes et qui est nécessaire dans le contexte de la banque de données. Le sexe et/ou le genre a en effet des conséquences en cas de contrôle de la personne par les services de police qui doivent prendre des dispositions spécifiques dans l'exécution de leurs missions, par exemple pour une fouille. Le sexe et/ou le genre est de plus une donnée nécessaire au moment de l'analyse des données (article 5, finalité d'analyse). L'analyse peut faire apparaître la nécessité de mener les actions appropriées et, le cas échéant, différenciées en fonction du genre. L'analyse permettra alors aussi de définir les priorités dans les actions à mener afin d'éviter que les personnes passent à des actes terroristes ou à de l'extrémisme pouvant mener au terrorisme. Il est bien entendu que si les personnes concernées sont très majoritairement de sexe et/ou de genre masculin, les actions de prévention s'orienteront prioritairement vers les hommes et devront s'organiser là où ceux-ci sont réceptifs aux actions, c'est-à-dire dans leurs lieux de vie habituels d'études, de sport ou de loisirs. Ce ne sont pas nécessairement les mêmes lieux où les jeunes filles ou les femmes pourraient être rencontrées. Dans le même contexte, l'analyse doit pouvoir déterminer si les implications dans la préparation ou l'accomplissement d'actes de terrorisme ou d'extrémisme pouvant mener au terrorisme sont différentes en fonction du sexe et/ou du genre. Il faut pour l'évaluation de la menace savoir si les femmes sont par exemple plus actives dans la préparation des actes terroristes alors que les hommes passent quant à eux plus facilement à l'acte, même de manière isolée. Le sexe et/ou le genre est donc dans ce cas également une donnée nécessaire.

5) la date, le lieu et le pays de naissance;

La date de naissance permet de déterminer l'âge des personnes concernées. L'année n'est pas suffisante dans la mesure où il faut aussi pouvoir déterminer le moment précis auquel ces personnes deviennent majeures car les mesures à prendre à l'égard des personnes physiques sont naturellement différentes selon que la personne est

3) het adres;

Op basis van het adres kan de persoon worden gelokaliseerd wanneer contact met hem moet worden opgenomen. Dat is niet het enige doel van dit gegeven. Het adres uit het Rijksregister bepaalt namelijk ook welke "lokale taskforce" bevoegd is en welke overheden en diensten moeten tussenkomen in het kader van preventie- of opvolgingshandelingen van de persoon.

4) het geslacht en/of het gender;

Het geslacht en/of het gender is een gegeven dat personen kenmerkt en dat noodzakelijk is in de context van de gegevensbank. Het heeft namelijk gevolgen indien de persoon wordt gecontroleerd door de politiediensten, die specifieke maatregelen moeten nemen in de uitvoering van hun opdrachten, bijvoorbeeld voor een fouillering. Het geslacht en/of het gender is des te meer een noodzakelijk gegeven op het ogenblik van de analyse van de gegevens (artikel 5, doeleinde inzake de analyse). Uit de analyse kan blijken dat het nodig is om gepaste acties te ondernemen, in voorkomend geval gedifferentieerd op basis van het gender. Op basis van de analyse kunnen dan ook de prioriteiten worden bepaald in de acties die moeten worden ondernomen om te voorkomen dat de personen overgaan tot terreurdaden of tot extremisme dat tot terrorisme kan leiden. Het spreekt voor zich dat, indien de overgrote meerderheid van de betrokkenen mannen zijn, de acties inzake de voorkoming in de eerste plaats op mannen gericht zijn en moeten worden georganiseerd waar die mannen er ontvankelijk voor zijn, dat wil zeggen op de gebruikelijke plaatsen waar ze studeren, sporten of hun vrije tijd doorbrengen. Het zijn niet noodzakelijkerwijs dezelfde plaatsen waar jonge meisjes of vrouwen zouden kunnen worden aangetroffen. In dezelfde context moet aan de hand van de analyse kunnen worden bepaald of de betrokkenheid in de voorbereiding of het plegen van terreurdaden of van daden van extremisme die tot terrorisme kunnen leiden, verschilt naargelang van het geslacht en/of het gender. Voor de dreigingsevaluatie moet men weten of vrouwen bijvoorbeeld actiever zijn in de voorbereiding van terreurdaden, terwijl mannen gemakkelijker overgaan tot daden, zelfs in hun eentje. In dat geval is het geslacht en/of het gender dus eveneens een noodzakelijk gegeven.

5) de geboortedatum, -plaats en het geboorteland;

De geboortedatum maakt het mogelijk de leeftijd van de betrokkenen te bepalen. Het jaar volstaat niet, aangezien ook het precieze moment waarop die personen meerderjarig worden, moet kunnen worden bepaald, omdat de maatregelen die moeten worden genomen ten aanzien van natuurlijke personen vanzelfsprekend

mineure ou majeure. C'est par exemple le cas pour les signalements nationaux et internationaux. Concernant le lieu et le pays de naissance, ils permettent d'établir le lien existant ou ayant existé avec la Belgique ou d'autres pays le cas échéant.

6) la nationalité;

La nationalité est importante dans le contexte des mesures à prendre dont celles de la compétence de l'Office des étrangers en ce qui concerne l'accès au territoire, le séjour, l'établissement et l'éloignement. On peut aussi penser à l'invalidation de passeports conformément au Code consulaire.

7) la description physique de la personne. Par exemple, indication de tatouage, etc.;

La description physique des personnes permet aux services de base et partenaires d'identifier, autrement que par le nom et le prénom, des personnes enregistrées dans la banque de données. Pratiquement, les services, et en particulier les services de police, peuvent être informés par des citoyens d'agissements étranges qui se sont passés dans leur quartier et impliquant des individus se rassemblant pour proférer des menaces à l'encontre de personnes d'une autre religion et pour encourager à des actions violentes, le cas échéant armées, à leur égard. Les citoyens qui prennent le soin de fournir cette information sont capables de donner une description physique des individus qui ont proféré les menaces et ont encouragé à l'action violente. Les informations récoltées peuvent alors être comparées aux données des descriptions physiques enregistrées dans la banque de données et une ou des correspondances pourraient permettre l'identification des participants ou de certains d'entre eux. Même si les correspondances ne donnent pas de certitude immédiate quant à l'identité, elles ouvrent une porte à des investigations complémentaires qui aboutiront ou non à une identification. Quel que soit le résultat il serait dommageable de ne pas pouvoir exploiter la banque de données notamment dans les circonstances expliquées ci-dessus.

8) des photos;

Compte tenu des multiples identités que les personnes concernées peuvent se donner, sur base ou non de documents d'identité réels ou falsifiés, le nom et le prénom, voire les alias, ne sont pas suffisants et il faut une quatrième donnée pour s'assurer de l'identité d'une personne. Cette quatrième donnée est la photo du visage ou de la silhouette de la personne. En travaillant

verschillen naargelang de persoon minderjarig of meerderjarig is. Dat is bijvoorbeeld het geval voor nationale en internationale seiningen. De geboorteplaats en het geboorteland maken het mogelijk de bestaande band of de band die heeft bestaan met België of in voorkomend geval met andere landen vast te stellen.

6) de nationaliteit;

De nationaliteit is van belang in de context van de te nemen maatregelen, waaronder die onder de bevoegdheid van de Dienst Vreemdelingenzaken op het gebied van toegang tot het grondgebied, verblijf, vestiging en verwijdering. Er kan ook worden gedacht aan de ongeldigverklaring van paspoorten overeenkomstig het Consulair Wetboek.

7) de fysieke beschrijving van de persoon. Bijvoorbeeld, vermelding van tatoeage, enz.;

De beschrijving van de persoon stelt de basis- en partnerdiensten in staat de in de gegevensbank geregistreerde personen op een andere wijze te identificeren dan via de naam en voornaam. In de praktijk kunnen de diensten, en in het bijzonder de politiediensten, door burgers op de hoogte worden gebracht van ongewone handelingen die zich voordoen in hun buurt, waarbij personen betrokken zijn die zich verzamelen om dreigingen te uiten ten aanzien van personen met een andere godsdienst en om aan te zetten tot gewelddadige acties, in voorkomend geval gewapend, ten aanzien van hen. De burgers die de moeite nemen om die informatie te verstrekken, kunnen een beschrijving geven van de personen die de dreigingen hebben geuit en hebben aangezet tot de gewelddadige actie. De verzamelde informatie kan dan worden vergeleken met de gegevens van de beschrijvingen die in de gegevensbank zijn geregistreerd en op basis van een of meer overeenkomsten zouden de deelnemers of sommigen van hen kunnen worden geïdentificeerd. Ook al bieden de overeenkomsten geen onmiddellijke zekerheid met betrekking tot de identiteit, zetten ze wel de deur open voor aanvullende onderzoeken die al dan niet tot een identificatie leiden. Ongeacht het resultaat zou het nadelig zijn om de gegevensbank niet te kunnen raadplegen, met name in de hierboven uiteengezette omstandigheden.

8) foto's;

Gelet op de verschillende identiteiten die de betrokkenen zich kunnen aanmeten, al dan niet op basis van echte of vervalste identiteitsdocumenten, volstaan de naam en voornaam, of zelfs de aliassen, niet en is een vierde gegeven nodig om zich te vergewissen van iemands identiteit. Dat vierde gegeven is de foto van het gezicht of het silhouet van de persoon. Via de

sur les réseaux sociaux on peut détecter des activités terroristes et d'extrémisme pouvant mener au terrorisme. Bien souvent, les personnes liées à ces activités montrent leur photo et un alias. Sur base de cette photo, il est possible d'établir un lien avec une photo enregistrée dans la banque de données et par cette voie identifier la personne. La photo permet aussi aux services de base et partenaires de reconnaître la personne et de s'assurer qu'ils parlent bien de la même personne lors des discussions entre eux dont en particulier durant la TFL. Enfin, après la recherche sur base de la description physique expliquée ci-dessus, la photo permet d'établir un "album de photos" qui peut être présenté au témoin afin qu'il puisse y avoir une reconnaissance et, cette fois, l'identification du ou des individus ayant proféré des menaces ou encouragé à la violence.

9) s'il échet, la référence dactyloscopique unique;

La référence dactyloscopique est le code identifiant de manière unique des empreintes digitales. Des empreintes prises à différents moments, si ce sont bien les mêmes, auront toutes ce code unique. Il ne s'agit donc pas de traiter des empreintes digitales elles-mêmes dans la banque de données mais seulement d'utiliser ce code unique. Ce code permet de savoir que des empreintes ont été prises pour l'entité concernée. Si cela s'avère nécessaire, il faut envisager une recherche dans la source authentique de gestion des empreintes pour plus de détails. Le code unique traité permet aussi d'établir d'éventuelles fausses identités. Cela se produit par exemple lorsque les mêmes empreintes renvoient vers des noms et prénoms différents. À nouveau, si on considère les finalités de la banque de données, il est essentiel de pouvoir établir de tels liens et renseigner que différentes identités correspondent aux mêmes empreintes.

Cela permet aussi de couvrir la situation de personnes non identifiées qui ne peuvent être signalées que sur base de référence dactyloscopique unique en vue de pouvoir identifier ces personnes. Il faut rappeler que dans le cadre de la banque de données commune T.E.R., il est essentiel que l'entité soit identifiée de manière certaine.

sociale netwerken kunnen terroristische activiteiten en extremisme dat tot terrorisme kan leiden, worden opgespoord. Vaak tonen de personen die banden hebben met die activiteiten hun foto en een alias. Op basis van die foto kan een link worden gelegd met een foto die in de gegevensbank is geregistreerd en op die manier kan de persoon worden geïdentificeerd. De foto stelt de basis- en partnerdiensten ook in staat de persoon te herkennen en zich ervan te vergewissen dat ze het wel degelijk over dezelfde persoon hebben tijdens de onderlinge besprekingen, in het bijzonder tijdens de LTF. Tot slot maakt de foto het, na de opzoeking op basis van de beschrijving die hierboven werd uiteengezet, mogelijk een "fotoalbum" op te stellen dat aan de getuige kan worden voorgelegd, zodat er herkenning kan plaatsvinden en de persoon of personen die dreigingen heeft/hebben geuit of heeft/hebben aangezet tot geweld deze keer kan/kunnen worden geïdentificeerd.

9) indien van toepassing, de unieke dactyloscopische referentie;

De dactyloscopische referentie is de code aan de hand waarvan vingerafdrukken op unieke wijze kunnen worden geïdentificeerd. Vingerafdrukken die op verschillende momenten zijn afgenomen, hebben allemaal die unieke code, indien het effectief dezelfde zijn. Het is dus niet de bedoeling om vingerafdrukken zelf te verwerken in de gegevensbank, maar om enkel die unieke code te gebruiken. Op basis van die code weet men dat er vingerafdrukken zijn afgenomen voor de betrokken entiteit. Indien dat noodzakelijk blijkt, moet een opzoeking in de authentieke bron voor het beheer van de vingerafdrukken worden overwogen voor meer details. De verwerkte unieke code maakt het tevens mogelijk om eventuele valse identiteiten vast te stellen. Dat gebeurt bijvoorbeeld wanneer dezelfde vingerafdrukken verwijzen naar verschillende namen en voornamen. Wederom is het, vanuit de doeleinden van de gegevensbank, van essentieel belang om dergelijke links te kunnen leggen en te vermelden dat verschillende identiteiten overeenkomen met dezelfde vingerafdrukken.

Dit betreft met name de situatie van niet-geïdentificeerde personen die alleen gesinaleerd kunnen worden op basis van de unieke dactyloscopische referentie om deze personen te kunnen identificeren. Er moet erop worden gewezen dat het in het kader van de gemeenschappelijke gegevensbank T.E.R. van wezenlijk belang is dat de entiteit met zekerheid wordt geïdentificeerd.

10) l'État civil;

Cette donnée complète les données administratives relatives à une entité. Elle permet de savoir si des mesures que l'on prendrait à l'égard de l'entité peut avoir des conséquences sur d'autres personnes en raison de liens du mariage ou d'autres situations d'état civil possibles. Il s'agit de pouvoir faire une analyse au cas par cas en prenant également en compte la situation familiale effective.

11) la situation familiale;

Cette rubrique reprend des informations relatives à certains membres de la famille également connus dans le cadre de la problématique FTF, propagandistes de haine (PH)... Seuls les membres de la famille possédant eux-mêmes un statut FTF, PH... peuvent dès lors être repris dans la banque de données. Cette relation mentionne, par exemple, qu'il s'agit du frère d'un autre FTF, de la veuve d'un FTF (présumé) mort. Afin de répondre à l'avis du Comité R du 13 juillet 2023 sur ce point (§ 24), il faut rappeler que les données à caractère personnel traitées dans la banque de données commune T.E.R. doivent d'une part être adéquates, pertinentes et non excessives au regard des missions visées à l'article 3, et des finalités de la banque de données et d'autre part, présenter un lien direct avec la finalité du traitement. L'explication données ci-avant vise à garantir cela.

12) la profession;

La profession est importante car certaines d'entre elles sont soumises à des autorisations préalables. Il est donc important de savoir si la profession exercée a fait l'objet d'une procédure d'autorisation et, dans ce cas, s'il ne faut pas dans certaines circonstances prévenir l'autorité compétente ayant délivré l'autorisation pour une évaluation à son niveau. Le suivi de la personne peut indiquer une évolution vers le terrorisme ou l'extrémisme pouvant mener au terrorisme et la TFL doit pouvoir exercer ses missions prévues à l'article 32, § 2, 3° en connaissant la profession. On devra savoir qu'un extrémiste potentiellement violent est armurier à titre de profession ou même au titre d'activité complémentaire. La vigilance sera de mise dès lors qu'une personne enregistrée comme prédicateur de haine exerce la profession d'éducateur.

Même lorsqu'elle ne fait pas l'objet d'une autorisation préalable, la profession est une donnée importante pour l'évaluation de la menace au cas par cas. C'est donc

10) de burgerlijke staat;

Dit gegeven vormt een aanvulling op de administratieve gegevens van een entiteit. Het maakt het mogelijk om in te schatten of de maatregelen die ten aanzien van de entiteit worden genomen in voorkomend geval gevolgen kunnen hebben voor andere personen, wegens een huwelijksband of andere mogelijke burgerlijke staten. Het doel is geval per geval een analyse te kunnen maken, eveneens rekening houdend met de daadwerkelijke gezinssituatie.

11) de gezinssituatie;

Deze rubriek bevat gegevens over bepaalde gezinsleden die eveneens bekend zijn in het kader van de FTF-problematiek, die bekend zijn als haatpropagandisten (HP's), enz. Enkel de gezinsleden die zelf het statuut van FTF, PH, enz. hebben, kunnen derhalve worden opgenomen in de gegevensbank. Voorbeelden van relaties zijn: broer van een andere FTF, weduwe van een (vermoedelijk) overleden FTF, enz. Teneinde tegemoet te komen aan het advies van Comité I van 13 juli 2023 in dat verband (§ 24) dient erop te worden gewezen dat de persoonsgegevens die in de gemeenschappelijke gegevensbank T.E.R. worden verwerkt ten eerste toereikend, ter zake dienend en niet overmatig moeten zijn in verhouding tot de opdrachten bedoeld in artikel 3, en de doeleinden van de gegevensbank, en ze ten tweede in rechtstreeks verband moeten staan met het doeleinde van de verwerking. De hierboven verstrekte toelichting beoogt dat te waarborgen.

12) het beroep;

Het beroep is een belangrijk gegeven omdat voor sommige beroepen een voorafgaande vergunning is vereist. Het is dan ook belangrijk te weten of voor het uitgeoefende beroep een vergunningsprocedure is doorlopen en, als dat het geval is, of in bepaalde omstandigheden de bevoegde overheid die de vergunning heeft afgegeven niet moet worden ingelicht met het oog op een evaluatie op haar niveau. De opvolging van de persoon kan uitwijzen dat er een evolutie is in de richting van terrorisme of extremisme dat tot terrorisme kan leiden en de LTF moet zijn opdrachten bedoeld in artikel 32, § 2, 3°, kunnen uitvoeren met kennis van het beroep. Het is noodzakelijk te weten of een potentieel gewelddadige extremist in hoofd- of in bijberoep wapenhandelaar is. Waakzaamheid is ook geboden wanneer een als haatpropagandist geregistreerde persoon als opvoeder werkt...

Ook wanneer er geen voorafgaande vergunning voor is vereist, blijft het beroep een belangrijk gegeven in het kader van de gevalsgewijze dreigingsevaluatie. Het is

l'analyse qui permet de déterminer si une profession exercée présente un risque eu égard à l'ensemble des données relatives à l'entité. On peut penser à l'État d'esprit de la personne concernée et sa volonté de s'en prendre à une catégorie déterminée de personnes avec lesquelles la personne concernée est régulièrement en contact professionnellement. Ce pourrait aussi être le cas d'une personne qui souhaite financer des actes terroristes et qui occupe un emploi lui permettant facilement de détourner des transactions financières...

13) les éléments liés à sa localisation;

Il est important de connaître les circonstances dans lesquelles une personne vit. L'adresse qui est enregistrée dans la banque de données doit être complétée par d'autres données de localisation comme, par exemple, l'adresse où se trouve la personne sans nécessairement y résider. Dans différents cas, il est en effet apparu qu'une personne n'occupait que très occasionnellement son domicile mais vivait en réalité ailleurs, parfois même en un lieu très éloigné de son domicile. Il est important que les adresses réelles ou effectives dont disposent les différents services soient mises en commun dans la banque de données. Comme les personnes concernées sont souvent très mobiles et qu'elles organisent des lieux de refuge où se protéger plus ou moins longtemps ou qu'elles occupent parfois aussi des biens sous-loués, il est nécessaire de disposer de différentes adresses dans la banque de données. Par exemple, on ne peut pas toujours déduire de l'adresse ou du quartier le type de situation dans laquelle se trouve une personne. En particulier, l'exemple du squat montre que ces données sont utiles pour fournir un cadre interprétatif précis de la situation de la personne.

Il faut aussi prendre en compte le fait qu'une personne pourrait elle-même renseigner des adresses différentes aux services avec lesquels elle est en contact. La police pourrait avoir une adresse pour d'éventuels contacts tandis qu'un service social recevrait lui une adresse totalement différente. La mise en commun de ces données dans la banque de donnée est donc fort importante.

14) moyens de communication;

Par moyens de communication, on entend les "identifiers", c'est-à-dire les moyens ou les données que la personne concernée utilise pour s'identifier ou accéder à l'internet, à de la messagerie ou aux réseaux sociaux. Il s'agit d'adresse mail, URL (*uniform resource locator*), IP ou DNS (*internet host*). Ces données sont nécessaires pour détecter les canaux utilisés par la personne concernée afin de diffuser, par exemple des messages appelant au terroriste, donnant des signaux

dus de l'analyse qui permet de déterminer si une profession exercée présente un risque eu égard à l'ensemble des données relatives à l'entité. On peut penser à l'État d'esprit de la personne concernée et sa volonté de s'en prendre à une catégorie déterminée de personnes avec lesquelles la personne concernée est régulièrement en contact professionnellement. Ce pourrait aussi être le cas d'une personne qui souhaite financer des actes terroristes et qui occupe un emploi lui permettant facilement de détourner des transactions financières...

13) elementen in verband met de locatie;

Het is van belang om te weten in welke omstandigheden een persoon leeft. Het in de gegevensbank geregistreerde adres moet worden aangevuld met andere locatiegegevens, bijvoorbeeld het adres waar de persoon zich bevindt zonder dat hij er noodzakelijkerwijs woont. In verschillende zaken is immers gebleken dat een persoon slechts heel af en toe op zijn woonplaats verbleef en in werkelijkheid elders woonde, soms zelfs zeer ver uit de buurt van zijn woonplaats. Het is belangrijk dat de echte of werkelijke adressen waarover de verschillende diensten beschikken in de gegevensbank worden gebundeld. Aangezien de betrokken personen vaak zeer mobiel zijn en schuilplaatsen inrichten waar ze voor korte of lange tijd veilig zijn of soms ook in onderverhuurde panden wonen, is het noodzakelijk om in de gegevensbank over verschillende adressen te beschikken. Zo kan men niet altijd uit het adres of de wijk afleiden in wat voor situatie een persoon zich bevindt. Met name het voorbeeld van verblijf in een kraakpand illustreert dat deze gegevens nuttig zijn om een interpretatiekader te scheppen over de situatie van de persoon in kwestie.

Er moet ook rekening worden gehouden met de mogelijkheid dat een persoon zelf verschillende adressen kan meedelen aan de diensten waarmee hij contact heeft. Zo zou de politie een bepaald kunnen hebben voor eventuele contacten, terwijl een sociale dienst een totaal ander adres kan krijgen. Het is dan ook zeer belangrijk dat die gegevens worden gebundeld in de gegevensbank.

14) communicatiemiddelen;

Onder communicatiemiddelen worden de "identifiers" verstaan, namelijk de middelen of de gegevens die de betrokken persoon gebruikt om zich te identificeren op of zich toegang te verschaffen tot het internet, e-maildiensten of de sociale netwerken. Het gaat om de volgende gegevens: e-mailadres, URL (*uniform resource locator*), IP-adres of DNS (*internet host*). Die gegevens zijn nodig voor het opsporen van de kanalen die de betrokken persoon gebruikt om bijvoorbeeld boodschappen

précis et sans équivoque de terrorisme ou d'extrémisme pouvant mener au terrorisme. Il s'agit aussi de mettre en commun des données qui permettent aux différents services d'exécuter leur mission mais aussi à la TFL d'évaluer les mesures appropriées comme le prévoit l'article 33, § 2, 13° et 14°.

Pour les mêmes raisons, d'autres adresses digitales pourront être enregistrées, par exemple, une adresse e-mail reliée à un compte Skype ou Facebook.

Enfin, comme il existe de nombreux sites Internet ou applications qui exigent un nom d'utilisateur ou un pseudo spécifique, ces "pseudos" seront aussi enregistrés dans la banque de données. Un numéro de téléphone est aussi une donnée intéressante pour les services de base et partenaires. Outre la possibilité de rentrer en contact avec les personnes concernées, le numéro de téléphone permet aussi à ces services de faire le lien avec d'autres numéros que ces services traitent dans le cadre de leur mission. Pour la police par exemple, dans une enquête, ce numéro pourrait montrer le lien de la personne concernée avec d'autres personnes suspectées d'avoir commis ou de vouloir commettre des délits ou des crimes. Cela déclencherait directement des réactions rapides dont l'information des autorités judiciaires afin de prendre les mesures pénales adéquates.

A. 2. Sont également traitées dans la banque de données commune T.E.R., les données relatives au nom, prénom, date de naissance et genre des enfants mineurs, biologiques ou adoptés d'un parent, personne physique qui y est enregistré comme *foreign terrorist fighter* qui séjourne ou a séjourné en zone de conflit djihadiste. Il ne s'agit ni de les reprendre dans la banque de données commune T.E.R. comme "entités" en tant que telles (ils ne sont donc pas repris à titre principal) ni d'enregistrer les enfants de toutes les entités enregistrées mais uniquement ceux qui séjournent ou ont séjournés en zone de conflit djihadiste. Ceci pour pouvoir mettre en place les mesures de protection et de suivi les plus appropriées en cas de retour. Comme indiqué plus haut, l'objectif est d'une part de pouvoir avoir un aperçu le plus précis possible des enfants qui sont sur zones de combat djihadiste et d'autre part, lors de leur retour, il est nécessaire de disposer des informations quant au lien qui existe avec un adulte dans le cadre du suivi socio-préventif de ses enfants.

te verspreiden waarin wordt opgeroepen tot terrorisme of die duidelijke en ondubbelzinnige signalen bevatten van terrorisme of extremisme dat tot terrorisme kan leiden. Het is ook de bedoeling de gegevens te bundelen die de verschillende diensten in staat stellen hun opdracht uit te voeren maar ook de LTF in staat stellen om te evalueren welke maatregelen passend zijn, als bedoeld in artikel 33, § 2, 13° en 14°.

Om dezelfde redenen kunnen andere digitale adressen worden geregistreerd: bijvoorbeeld een e-mailadres dat gekoppeld is aan een Skype- of Facebook-account.

Tot slot bestaan er tal van websites en applicaties waarvoor een gebruikersnaam of een specifiek pseudo-niem nodig is. Die "pseudos" zullen eveneens worden geregistreerd in de gegevensbank. Ook een telefoonnummer is een interessant gegeven voor de basis- en de partnerdiensten. Het telefoonnummer biedt niet alleen de mogelijkheid om in contact te treden met de betrokken personen, het biedt de voornoemde diensten ook de mogelijkheid om verbanden te leggen met andere nummers die ze verwerken in het kader van hun opdracht. Voor de politie bijvoorbeeld, kan het telefoonnummer in het kader van een onderzoek de band aantonen tussen de betrokken persoon en andere personen die ervan worden verdacht wanbedrijven of misdaden te hebben gepleegd of te willen plegen. Zulks zou onmiddellijk leiden tot snelle reacties, waaronder het informeren van de gerechtelijke overheden teneinde de passende strafrechtelijke maatregelen te nemen.

A. 2. De gegevens inzake de naam, de voornaam, de geboortedatum en het gender van de biologische of geadopteerde minderjarige kinderen van een ouder, die een natuurlijke persoon, is die in de gemeenschappelijke gegevensbank T.E.R. is opgenomen als *foreign terrorist fighter* die in een jihadistisch conflictgebied verblijft of heeft verbleven, worden daarin eveneens verwerkt. Het is niet de bedoeling om ze in de gemeenschappelijke gegevensbank T.E.R. op te nemen als "entiteiten" als dusdanig (in de hoedanigheid van "hoofdentiteit" dus), en ook niet om de kinderen van alle opgenomen entiteiten ambtshalve erin op te nemen, maar louter om diegenen die in een jihadistisch conflictgebied verblijven of hebben verbleven erin op te nemen. Doel daarvan is om de geschikteste beschermings- en opvolgingsmaatregelen te kunnen nemen in het geval van terugkeer. Zoals hierboven aangegeven is het ten eerste de bedoeling om een zo nauwkeurig mogelijk overzicht te kunnen hebben van de kinderen die in een jihadistisch strijdgebied verkeren, en is het ten tweede nodig om bij hun terugkeer over informatie te beschikken over de bestaande band met een volwassene in het kader van de sociopreventieve opvolging van diens kinderen.

Ce n'est donc que dans ces cas spécifiques qu'un enfant est traité dans les données relatives à son parent, pour une finalité de protection, de suivi et de réintégration.

A. 3. Certains catégories particulières de données à caractères personnel au sens de l'article 9. 1) du RGPD et de l'article 34 de la loi relative à la protection des données seront également reprises dans la banque de données commune T.E.R. Il s'agit des suivantes: celles qui révèlent de l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé.

Concernant les catégories particulières de données à caractère personnel précitées, leur traitement est nécessaire et important pour comprendre le contexte lié à la personne concernée. Par exemple:

i. les données à caractère personnel qui révèlent l'origine ethnique;

Le fait de connaître l'origine ethnique d'une personne peut permettre de vérifier certaines informations et ainsi confirmer ou informer certaines hypothèses. Exemple: l'appartenance d'une personne à l'ethnie tadjik permet de déduire qu'il y a peu de chance qu'elle soit pro-taliban;

ii. les opinions politiques;

Dans le cadre du suivi des extrémistes de gauche ou de droite, il est important de connaître leur idéologie (qui est fortement liée à leur opinion politique). Il est important de savoir si une propagandiste de haine propage une idéologie de droite ou de gauche et même de quel type de droite ou de quel type de gauche. Exemple: l'enregistrement de ces informations peut permettre d'identifier d'éventuelles cibles de la personne suivie dans la banque de données commune T.E.R.

iii. les convictions religieuses ou philosophiques;

Dans les cas d'extrémisme et de terrorisme religieux, il est important de connaître la conviction religieuse de l'intéressé notamment pour identifier d'éventuelles cibles de l'intéressé. Exemple: un chiite ne va pas avoir les mêmes cibles que des sunnites. Savoir qu'une personne est salafiste madkhalite ou jihadiste a aussi un impact important sur l'évaluation qui peut être faite de la menace.

De gegevens van een kind worden dus enkel in die specifieke gevallen verwerkt in de gegevens betreffende zijn ouder, met het oog op bescherming, opvolging en re-integratie.

A. 3. Bepaalde bijzondere categorieën van persoonsgegevens in de zin van artikel 9. 1) van de GDPR en artikel 34 van de wet op de gegevensbescherming zullen ook in de gemeenschappelijke gegevensbank T.E.R. worden opgenomen. Dit zijn de volgende: de etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, de biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, gegevens over gezondheid van een natuurlijke persoon.

Met betrekking tot voornoemde bijzondere categorieën van persoonsgegevens is de verwerking ervan noodzakelijk en belangrijk om de context die verband houdt met de betrokken persoon te begrijpen. Bijvoorbeeld:

i. de persoonsgegevens waaruit de etnische afkomst kan afgeleid worden;

Kennis van iemands etnische afkomst kan helpen om bepaalde informatie te verifiëren en zo bepaalde veronderstellingen te bevestigen of te onderbouwen. Voorbeeld: Als een persoon een etnische Tadzjiek is, kan worden afgeleid dat het onwaarschijnlijk is dat hij of zij pro-Taliban is.

ii. de politieke opvattingen;

Bij het volgen van linkse of rechtse extremisten is het van belang hun ideologie te kennen (die sterk samenhangt met hun politieke opvattingen). Het is belangrijk te weten of een haatpropagandist een rechtse of linkse ideologie verspreidt, en zelfs wat voor soort rechtse of linkse ideologie. Voorbeeld: de registratie van deze informatie kan helpen om in de gemeenschappelijke gegevensbank T.E.R. mogelijke doelwitten van de gecontroleerde persoon te identificeren.

iii. de godsdienstige of levensbeschouwelijke overtuiging;

In gevallen van religieus extremisme en terrorisme is het van belang de godsdienstige overtuiging van de betrokkene te kennen, met name om mogelijke doelwitten van de betrokkene te identificeren. Een sjiiet heeft bijvoorbeeld niet dezelfde doelen als een soenniet. De wetenschap dat een persoon een madkhalitische salafist of een jihadist is, heeft ook een belangrijke invloed op de dreigingsbeoordeling die kan worden gemaakt.

Dans son avis n° 97/2023 du 16 juin 2023, l'Autorité de protection des données s'interroge sur la nécessité de traiter également les convictions philosophiques (§ 101). Or, cette notion fait partie intégrante de la définition d'extrémisme visé à l'article 8, 1°, c), de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité: "les conceptions ou les visées racistes, xénophobes, anarchistes, nationalistes, autoritaires ou totalitaires, qu'elles soient à caractère politique, idéologique, confessionnel ou philosophique, contraires, en théorie ou en pratique, aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux autres fondements de l'État de droit en ce compris le processus de radicalisation.". Cette définition constitue la base de travail des services de base et des services partenaires comme le précise l'article 3 du projet.

À titre d'exemples de convictions philosophiques justifiant la nécessité de traiter ces données, on peut citer le survivalisme qui ne constitue ni une conviction politique, ni une conviction religieuse, ou encore l'extrémisme de droit qui n'est pas nécessairement liées à une conviction politique.

iv. des données biométriques aux fins d'identifier une personne physique de manière unique;

Ainsi par exemple, les données biométriques permettront notamment de couvrir la situation de personnes non identifiées qui ne peuvent être signalées que sur cette base en vue de pouvoir être identifiées. On peut ainsi imaginer le cas d'un *foreign terrorist fighter* catégorie 1 qui voudrait revenir en Belgique avec une fausse identité. Le partage de données biométriques dans la banque de données commune T.E.R. pourrait permettre aux différents services compétents d'identifier la personne sous sa fausse identité. Il faut rappeler que dans le cadre de la banque de données commune T.E.R., il est essentiel que l'entité soit identifiée de manière certaine. Pour répondre à l'avis du 13 juillet 2023 du Comité R concernant ces données (§ 24), l'ensemble des données biométriques sont visées afin que les services puissent introduire les données biométriques qu'elles auraient à leur disposition afin d'identifier l'entité de manière certaine. Par exemple, un service étranger transmet les données biométriques présentes sur un CEM (captured enemy material). Il faut pouvoir comparer ces données.

In advies nr. 97/2023 van 16 juni 2023 heeft de Gegevensbeschermingsautoriteit vragen bij het noodzakelijke karakter van de verwerking van levensbeschouwelijke overtuigingen (§ 101). Dat begrip maakt evenwel volledig deel uit van de omschrijving van extremisme bedoeld in artikel 8, 1°, c), van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten: "racistische, xenofobe, anarchistische, nationalistische, autoritaire of totalitaire opvattingen of bedoelingen, ongeacht of ze van politieke, ideologische, confessionele of filosofische aard zijn, die theoretisch of in de praktijk strijdig zijn met de beginselen van de democratie of de mensenrechten, met de goede werking van de democratische instellingen of andere grondslagen van de rechtsstaat. Hieronder wordt ook het radicaliseringsproces begrepen". Deze definitie ligt ten grondslag van de werkzaamheden van de basisdiensten en partnerdiensten zoals gepreciseerd in artikel 3 van het ontwerp.

Levensbeschouwelijke overtuigingen waarvan de gegevens terecht mogen worden verwerkt, zijn bijvoorbeeld survivalisme (dat noch een politieke, noch een religieuze overtuiging is) en extreemrechts (dat niet per se verband hoeft te houden met een politieke opvatting).

iv. biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon;

Biometrische gegevens kunnen bijvoorbeeld worden gebruikt wanneer niet-geïdentificeerde personen alleen kunnen worden geseind op deze basis, teneinde die personen te kunnen identificeren. Men kan zich het geval voorstellen van een *foreign terrorist fighter* van categorie 1 die met een valse identiteit naar België wil terugkeren. Het delen van de biometrische gegevens in de gemeenschappelijke gegevensbank T.E.R. zou de verschillende bevoegde diensten in staat kunnen stellen de persoon onder zijn valse identiteit te identificeren. Er moet erop worden gewezen dat het in het kader van de gemeenschappelijke gegevensbank T.E.R. van wezenlijk belang is dat de entiteit met zekerheid wordt geïdentificeerd. In antwoord op het advies van 13 juli 2023 van Comité I aangaande dergelijke gegevens (§ 24): alle biometrische gegevens worden beoogd, zodat de diensten de biometrische gegevens te hunner beschikking kunnen invoeren om de entiteit met zekerheid te identificeren, zoals het geval van een buitenlandse dienst die de aanwezige biometrische gegevens op CEM (captured enemy material) doorgeeft. Die gegevens moeten kunnen worden vergeleken.

v. les données concernant la santé;

La connaissance d'éléments de santé peut permettre de vérifier certaines informations ou de déterminer les capacités de quelqu'un. En effet, une particularité physique peut avoir une implication sur son comportement. Exemple: lors de l'attaque de Hassakeh par IS, le sort des FTF belges qui s'y trouvaient n'était pas clair. Il semblait cependant directement improbable qu'un unijambiste puisse s'être évadé dans cet état. Autre exemple: une FTF belge à Damas se trouve en chaise roulante; la connaissance de cette information permet de quasiment exclure un retour clandestin en Belgique. De même, savoir qu'une personne est en fin de vie, et donc "prête à tout", est une information importante pour évaluer la menace qu'elle représente.

L'état mental, les traits majeurs de personnalité et les antécédents d'une entité sont aussi des données essentielles pour évaluer la menace qu'elle pourrait représenter. Il y a lieu de pouvoir apprécier le risque d'atteinte à l'intégrité physique et psychique de tiers. Il ne faut pas perdre de vue que les informations sont traitées dans le contexte de formes extrêmement graves de criminalité: le terrorisme et l'extrémisme lorsqu'il peut mener au terrorisme. Les données relatives à la santé sont donc traitées avec les autres données disponibles dans la perspective de l'évaluation de l'OCAM portant sur la menace que représente une entité. À son niveau, même si les données relatives à la santé sont intégrées dans l'évaluation de la menace à laquelle elle a accès, la Task Force Locale a besoin de ces données pour examiner les mesures les plus appropriées à prendre en fonction de la situation dans laquelle la personne se trouve. On est en effet confronté à un problème différent selon que la personne est incarcérée ou non. À cette fin et pour tenir informés les services membres de la TFL, la Direction générale des Etablissements pénitentiaires donnent régulièrement aux services de base des informations concernant les troubles mentaux des entités enregistrées dans la banque de données. Il s'agit souvent du comportement pendant l'incarcération mais aussi de l'évolution de ce comportement et du résultat d'entretiens entre la personne concernée et des médecins, dont les psychiatres. C'est pour ces raisons qu'il faut pouvoir traiter ces données dans la banque de données. À noter que si les services membres de la Task Force ne sont pas en mesure de prendre à leur niveau les bonnes mesures, la Task Force doit pouvoir alerter les autorités compétentes pour celles-ci. Cette alerte fait partie des missions que la loi confie à la TFL.

En dehors de l'analyse par la Task Force, il faut aussi que les services d'intervention de première ligne puissent

v. de gegevens betreffende de gezondheid;

Kennis van gezondheidselementen kan worden gebruikt om informatie te verifiëren of iemands capaciteiten vast te stellen. Een fysieke eigenschap kan immers gevolgen hebben voor het gedrag. Toen IS bijvoorbeeld Hassakeh aanviel, was het lot van de Belgische FTF's daar onduidelijk. Het leek echter hoogst onwaarschijnlijk dat een man met één been in deze toestand kon ontsnappen. Een ander voorbeeld: een Belgische FTF in Damascus zit in een rolstoel; kennis van deze informatie maakt het mogelijk een clandestiene terugkeer naar België bijna uit te sluiten. Ook de wetenschap dat een persoon aan het eind van zijn leven is, en dus "tot alles bereid" is, is belangrijke informatie voor de beoordeling van de bedreiging die hij vormt.

De geestestoestand, de belangrijkste persoonlijkheidskenmerken en de antecedenten van een entiteit zijn ook essentiële gegevens voor de beoordeling van de bedreiging die de entiteit zou kunnen vormen. Het risico op aantasting van de fysieke en psychische integriteit van derden moet kunnen worden beoordeeld. Er mag niet uit het oog worden verloren dat de gegevens worden verwerkt in de context van extreem ernstige vormen van criminaliteit: terrorisme en extremisme wanneer het kan leiden tot terrorisme. De gegevens over de gezondheid worden dus samen met de andere beschikbare gegevens verwerkt in het perspectief van de dreigingsevaluatie van het OCAD betreffende een entiteit. Hoewel de gegevens over de gezondheid worden opgenomen in de dreigingsevaluatie waartoe de lokale taskforce toegang heeft, heeft die taskforce op zijn niveau die gegevens nodig om te onderzoeken welke maatregelen het best worden genomen in het licht van de toestand waarin de persoon zich bevindt. Het probleem is immers anders naargelang de persoon al dan niet is opgesloten. Daartoe en om de leden van de LTF op de hoogte te houden, verschaft het directoraat-generaal Penitentiare Inrichtingen de basisdiensten regelmatig informatie over de psychische problemen van de in de gegevensbank geregistreerde entiteiten. Die informatie betreft vaak het gedrag tijdens de opsluiting, maar ook de evolutie van dat gedrag en het resultaat van gesprekken tussen de betrokken persoon en artsen, onder wie de psychiaters. Om die redenen moeten de gegevens in kwestie kunnen worden verwerkt in de gegevensbank. Er moet worden opgemerkt dat wanneer de leden van de taskforce op hun niveau niet de juiste maatregelen kunnen nemen, de taskforce de voor die maatregelen bevoegde overheden moet kunnen waarschuwen. Die waarschuwing maakt deel uit van de opdrachten die de wet toevertrouwt aan de LTF.

Los van de analyse door de taskforce, moeten ook de eerstelijnsinterventiediensten de bevoegde overheden op

informer les autorités compétentes lorsqu'ils constatent sur la voie publique ou lors de contacts dans le cadre de leurs missions des attitudes, un discours ou des comportements peu adaptés ou peu adéquats d'entités connues de la banque de données qui peuvent mettre en danger l'intégrité psychique ou physique d'autrui. Ainsi la police qui détecte des propos incohérents et menaçants d'une personne doit pouvoir faire part dans ses rapports aux autorités compétentes d'antécédents problématiques. Les données disponibles dans la banque de données permettent de préciser le niveau de dangerosité et le caractère récurrent de celle-ci. Dès lors qu'il s'agit d'entités enregistrées dans la banque de données dans une matière aussi sérieuse que le terrorisme et l'extrémisme pouvant mener au terrorisme, il est primordial pour la sécurité des premiers intervenants et des citoyens qu'il y ait une circulation optimale des données relatives à la santé, nécessaires à l'appréciation de la dangerosité de l'entité en question. Outre la santé mentale, les antécédents et les données de personnalité, il faut aussi pouvoir traiter les données relatives aux troubles de l'usage des substances (alcool, drogues et médicaments). En effet, ces substances peuvent altérer sérieusement l'État mental de l'entité avec un risque significatif de passage à l'acte. Ces données revêtent aussi un caractère important au moment où des personnes suivies sur le plan psychiatrique ou psychologique dans un établissement pénitentiaire quittent cet établissement après l'exécution complète de leur peine. Le suivi mis en place dans le monde carcéral est alors interrompu mais les problèmes peuvent subsister. Il convient de s'assurer d'une continuité des soins pour les entités avec une problématique mentale ou d'assuétudes. Celles-ci doivent en effet continuer à être discutées au sein de la TFL afin d'examiner les possibilités légales de leur suivi et des mesures à prendre en cas de dégradation de leur situation.

Pour rappel, ces dernières données sont traitées uniquement dans le but de comprendre le contexte médical somatique et mental lié à la personne concernée, en lien direct avec les finalités visées à l'article 5, alinéa 2, ainsi que pour assurer la sécurité et protéger l'intégrité psychique et physique de toute personne susceptible d'entrer en contact avec les personnes concernées dans le cadre de l'intervention des autorités compétentes, en ce compris les prestataires de soins. Lorsque des données relatives à la santé sont traitées, il est mentionné si ces données proviennent ou non de professionnels de soins de la santé. Le traitement de données relatives à la santé visé dans cet article n'a jamais pour conséquence de contraindre les personnes concernées à se soumettre à des examens médicaux (art. 6, § 2, al. 2). En outre,

de hoogte kunnen brengen wanneer ze op de openbare weg of tijdens contacten in het kader van hun opdrachten weinig gepaste houdingen, uitspraken of gedragingen vaststellen bij entiteiten die in de gegevensbank bekend zijn en de fysieke of psychische integriteit van anderen in gevaar kunnen brengen. Zo moet de politie, wanneer zij onsamenhangende en bedreigende uitspraken van een persoon opvangt, problematische antecedenten kunnen melden in haar verslagen aan de bevoegde overheden. Aan de hand van de in de gegevensbank beschikbare gegevens kan worden verduidelijkt hoe groot het gevaar is en hoe vaak het zich voordoet. Aangezien het gaat om entiteiten die in de gegevensbank zijn geregistreerd in het kader van danig ernstige aangelegenheden als terrorisme en extremisme dat tot terrorisme kan leiden, is het voor de veiligheid van de eerste intervenanten en de burgers van primordiaal belang dat er een optimale doorstroming is van de gezondheidsgegevens die noodzakelijk zijn om te beoordelen hoe gevaarlijk de entiteit in kwestie is. Naast de gegevens betreffende de geestelijke gezondheid, de antecedenten en de persoonlijkheid moet het ook mogelijk zijn om de gegevens betreffende problemen met het gebruik van stoffen (alcohol, drugs en geneesmiddelen) te verwerken. Verslavende stoffen kunnen immers de geestestoestand van de entiteit ernstig beïnvloeden, met een significant hoger risico op terreurdaden tot gevolg. De gegevens in kwestie zijn ook belangrijk wanneer personen die in een penitenciaire inrichting psychologisch of psychiatisch worden opgevolgd die inrichting verlaten na de volledige uitvoering van hun straf. De opvolging waarin in de gevangenisomgeving wordt voorzien, wordt dan stopgezet, maar de problemen kunnen er nog steeds zijn. Voor entiteiten met een geestesstoornis of een verslavingsproblematiek dient een continuïteit van de zorgverlening te worden gewaarborgd. Zij moeten binnen LTF immers blijven besproken worden om te onderzoeken wat de wettelijke mogelijkheden zijn om hen op te volgen en om te bepalen welke maatregelen moeten worden genomen wanneer hun toestand verslechtert.

Ter herinnering, deze laatste gegevens worden enkel verwerkt met het oog op het begrijpen van de medische somatische en geestelijke omstandigheden waarin de betrokken persoon zich bevindt, in rechtstreeks verband met de in artikel 5, lid 2, genoemde doeleinden, evenals om de veiligheid te garanderen en de psychische en fysieke integriteit te beschermen van elke persoon die in contact zou kunnen komen met de betrokken personen in het kader van de interventie door de bevoegde overheden, waaronder zorgverleners. Wanneer gezondheidsgegevens worden verwerkt, wordt vermeld of deze gegevens al dan niet afkomstig zijn van beroepsbeoefenaren in de gezondheidszorg. De verwerking van gezondheidsgegevens waarnaar in dit artikel wordt verwezen, heeft nooit als gevolg de betrokkenen te laten

comme le rappelle l'Autorité de protection des données dans son avis n° 97/2023 du 16 juin 2023, le traitement des données relatives à la santé ne se confond pas avec la communication d'un dossier médical à laquelle les articles 9 et 10 de la loi du 22 août 2002 relative aux droits du patient continuent à s'appliquer (§ 100). Cela répond également à la préoccupation du Comité R (avis du 13 juillet 2023, § 23).

Dans l'intérêt de la personne concernée et de celle des prestataires de soins, il est parfois essentiel de connaître l'État de dangerosité d'un individu. C'est pourquoi, il est prévu que le service de base qui est en contact avec le prestataire de soins lui communique données concernant la santé nécessaires et les données issues de l'évaluation de la menace relatives à la dangerosité de la personne (art. 6, § 2, al. 3). En réponse à ce que recommande le C.O.C. dans son avis du 20 juin 2023, il est préférable de ne pas prévoir une communication nécessairement écrite de ces informations. En effet, cette disposition entend s'appliquer à des situations d'urgence qui nécessitent dès lors une communication rapide et donc orale. Par ailleurs, une communication écrite de ces informations au prestataire de soins peut entraîner un problème de sécurité dans la mesure où cet écrit pourrait être divulgué à des personnes non autorisées ou se perdre dans la nature. Néanmoins, cette communication à l'égard d'un prestataire de soin devra faire l'objet de précision dans une circulaire ministérielle.

À ce sujet encore, l'Autorité de protection des données, dans son avis n° 97/2023 du 16 juin 2023, estime qu'il convient de déterminer l'obligation à laquelle le personnel médical serait soumise sur base de ces informations (§ 50). Or, cette communication au prestataire de soin vise à lui permettre d'agir dans la sphère de compétence qui est la sienne, selon les mesures habituelles et adéquates qu'il prend à l'égard d'une telle situation. Il n'appartient dès lors pas aux services de police ou autres de dire au corps médical la manière dont il doit effectuer son travail.

Le traitement de toutes les catégories particulières de données à caractère personnel précitées est assorti des garanties appropriées exigées par la loi relative à la protection des données. En effet, les données contenues dans la banque de données commune T.E.R. sont accessibles sur base de différents droits d'accès que le Roi va donner aux services énumérés dans la loi sur la base du respect des principes d'adéquation, de pertinence et du caractère non excessif, dans le cadre de l'exercice de leurs missions visées à l'article 3 et conformément aux finalités de l'article 5, alinéa 2. Cela

onderwerpen aan medische onderzoeken (art. 6, § 2, tweede lid). Zoals de Gegevensbeschermingsautoriteit in advies nr. 97/2023 van 16 juni 2023 opmerkt, is de verwerking van gegevens met betrekking tot de gezondheid niet hetzelfde als de mededeling van een medisch dossier, waarop de artikelen 9 en 10 van de wet van 22 augustus 2002 betreffende de rechten van de patiënt van toepassing blijven (§ 100). Dat komt eveneens tegemoet aan de bezorgdheid van Comité I (advies van 13 juli 2023, § 23).

In het belang van de betrokken persoon en van de zorgverleners is het soms essentieel om te weten hoe gevaarlijk iemand is. Daarom wordt erin voorzien dat de basisdienst die in contact staat met de zorgverlener hem de nodige gegevens over gezondheid en de gegevens die afkomstig zijn van de dreigingsevaluatie met betrekking tot de gevaarlijkheid van de betrokken persoon meedeelt (art. 6, § 2, derde lid). In antwoord op wat het COC aanbeveelt in het advies van 20 juni 2023, verdient het de voorkeur niet te bepalen dat die communicatie van de informatie noodzakelijkerwijs schriftelijk dient te gebeuren. Deze bepaling is immers ook van toepassing op spoedeisende situaties, waarvoor bijgevolg snel en dus mondeling moet worden gecommuniceerd. Bovendien kan het schriftelijk communiceren van dergelijke informatie aan de zorgverlener aanleiding geven tot een veiligheidsprobleem, omdat die tekst aan onbevoegden zou kunnen worden bekendgemaakt of zoek zou kunnen raken. Niettemin moet deze communicatie ten aanzien van een zorgverlener nader worden verduidelijkt in een ministeriële omzendbrief.

Ook daarover meent de Gegevensbeschermingsautoriteit in advies nr. 97/2023 van 16 juni 2023 dat er moet worden bepaald welke verplichting van toepassing is op de medische staf op basis van die informatie (§ 50). Door de communicatie aan de zorgverlener kan hij handelen binnen zijn eigen bevoegdheid volgens de gangbare en passende maatregelen die hij in een dergelijke situatie neemt. Het is derhalve niet de taak van de politiediensten of van anderen om medische personeelsleden te zeggen hoe ze hun werk moeten doen.

Voor de verwerking van alle bovengenoemde bijzondere categorieën van persoonsgegevens gelden de passende, bij de gegevensbeschermingswet opgelegde waarborgen. De gegevens in de gemeenschappelijke gegevensbank T.E.R. zijn namelijk toegankelijk op basis van verschillende toegangsrechten die de Koning de in de wet opgesomde diensten zal verlenen op basis van de inachtneming van de principes van toereikendheid, relevantie en de niet-bovenmatige aard in het kader van de uitoefening van hun opdrachten bedoeld in artikel 3 en overeenkomstig de doeleinden van artikel 5,

visé donc le principe du besoin d'en connaître. En outre, chaque service devra identifier les membres de son personnel autorisés à exercer les droits d'accès à la banque de données commune T.E.R. et devra transmettre une liste de ces personnes au gestionnaire qui gère les accès. Cette liste pourra, le cas échéant, être mise à la disposition du délégué à la protection des données et au responsable opérationnel dans le cadre de leurs missions respectives. Il est également précisé que les membres du personnel doivent être titulaires d'une habilitation de sécurité de niveau "secret", pour accéder à la banque de données commune T.E.R.

A. 4. Seront également traitées dans la banque de données commune T.E.R.:

i. les données sur les formations suivies;

Il peut s'agir d'une formation dans le cadre du terrorisme ou du radicalisme ou de l'extrémisme pour acquérir des connaissances pratiques ou, à l'inverse, des formations suivies pour s'intégrer dans la société et retrouver un emploi.

ii. les données relatives à la situation financière;

Il s'agit d'un élément d'évaluation permettant de savoir par exemple si la personne rassemble de l'argent pour organiser des départs de personnes vers des zones de conflit, ou cherche à acquérir des fonds et contracte des dettes auprès d'établissements bancaires par exemple.

iii. les données relatives aux fréquentations à risque;

Ces données sont destinées à obtenir des informations sur le système de normes et valeurs de l'entité ainsi que sur le type de personne ou lieu qu'elle fréquente. Il ne s'agit nullement d'enregistrer d'autres identités que la personne déjà enregistrée dans la banque de données commune T.E.R. Ce type de données permettra par exemple de savoir si l'entité fréquente un milieu ou un lieu qui propage des idéologies extrémistes ou au contraire, s'éloigne de ce type de milieu ou de lieu ou encore, si elle a des contacts ou fréquente à nouveau des milieux interlopes. Ces informations peuvent aussi découler des contacts tenus avec les CSIL-R ou des TFL. En réponse au Comité R dans son avis du 13 juillet 2023 (§ 24), on peut indiquer qu'il est important de savoir qu'un extrémiste fréquente une librairie d'extrême gauche ou encore qu'une entité fréquente désormais une mosquée non radicalisante. Ces éléments permettent d'avoir des informations à charge ou à décharge de l'entité.

tweede lid. Dit beoogt dus het principe van de behoefte om te kennen. Voorts zal elke dienst moeten identificeren welke van zijn personeelsleden gemachtigd zijn om de toegangsrechten tot de gemeenschappelijke gegevensbank T.E.R. uit te oefenen en een lijst van die personen moeten bezorgen aan de beheerder van de toegangen. Die lijst kan, in voorkomend geval, ter beschikking worden gesteld van de functionaris voor gegevensbescherming en van de operationeel verantwoordelijke in het kader van hun respectieve opdrachten. Er wordt ook gepreciseerd dat de personeelsleden houder moeten zijn van een veiligheidsmachtiging van het niveau "geheim" om toegang te kunnen krijgen tot de gemeenschappelijke gegevensbank T.E.R.

A. 4. Onderstaande gegevens zullen ook in de gemeenschappelijke gegevensbank T.E.R. worden verwerkt:

i. gegevens over gevolgde opleidingen;

Dit kan een opleiding zijn in het kader van terrorisme of radicalisme of extremisme om praktische kennis te verwerven of, omgekeerd, een opleiding die wordt gevolgd om in de samenleving te integreren en een baan te vinden.

ii. gegevens over de financiële positie;

Dit is een beoordeling van de vraag of de persoon geld inzamelt om vertrek naar conflictgebieden te organiseren, of probeert geld te verwerven en schulden te maken bij bijvoorbeeld financiële instellingen.

iii. de gegevens met betrekking tot risicovolle verplaatsingen;

Deze gegevens zijn bedoeld om informatie te verschaffen over de normen en waarden van de entiteit en het soort mensen of plaatsen dat zij bezoekt. Er is geen sprake van het registreren van andere identiteiten dan de persoon die reeds in de gemeenschappelijke gegevens T.E.R. is geregistreerd. Met dit soort gegevens kan bijvoorbeeld worden nagegaan of de entiteit een omgeving of plaats bezoekt die extremistische ideologieën propageert of zich juist van dit soort omgeving of plaats distantieert dan wel of contacten heeft of teruggaat naar de onderwereld. Deze informatie kan ook worden afgeleid uit contacten met de LIVC of de TFL. In antwoord op het advies van 13 juli 2023 van Comité I (§ 24) kan worden vermeld dat het belangrijk is om te weten of een extremist vaak naar een extreemlinkse boekhandel gaat of dat een entiteit nu een niet-radicaliserende moskee bezoekt. Zo heeft men informatie à charge en à décharge over de entiteit ter beschikking.

iv. les données relatives aux absences de réponse aux convocations de l'autorité;

Par exemple, il pourrait être intéressant de savoir qu'une personne, membre de la banque de données commune T.E.R., suivie par les maisons de justice, ne vient pas à ses rendez-vous ou ne répond pas au rappel des assistants de Justice.

v. les moyens de transport;

Les moyens de transport sont également enregistrés.

Il s'agit des moyens de transport utilisés par la personne concernée. Par conséquent, cette catégorie ne se limite pas au moyen de transport dont elle est propriétaire, mais peut également concerner la voiture de la mère, d'un(e) ami(e) etc. Il ne s'agit cependant pas du moyen de transport dans lequel l'entité est régulièrement passagère. Si l'entité utilise uniquement les transports en commun, cet élément peut également être mentionné dans la banque de données.

L'important pour les services de base et partenaires est de connaître le type de moyens de transport, sa marque et sa couleur ainsi que son numéro d'immatriculation. Ces données permettent de mettre en relation des différentes informations. Si un moyen de transport est par exemple vu et son numéro relevé lors d'agissements suspects à proximité d'un aéroport, d'une gare, d'une ambassade ou tout autre point névralgique en Belgique, il faut pouvoir vérifier si le véhicule en question est un véhicule utilisé par une entité enregistrée dans la banque de données. En cas de correspondance entre la plaque relevée et une plaque enregistrée dans la banque de données, il est évident que l'information relative aux agissements suspects prend une tout autre importance avec des investigations pouvant être orientées vers l'entité concernée et des mesures de protection idoines des lieux concernés par les agissements suspects. Dans l'exemple qui précède, on parlait du principe que le véhicule avait été vu au moment des agissements suspects mais on peut aussi évoquer comme situation similaire la détection de la plaque d'immatriculation par un système ANPR disposé à proximité du lieu des agissements suspects ou même un peu plus loin et la recherche ensuite de la plaque dans la banque de données commune. Il est important d'autre part de savoir si l'entité utilise fréquemment des moyens de transport différents ou des véhicules de location afin de réfléchir, en commun, sur la raison de ces changements ou de l'utilisation de véhicules de location.

iv. gegevens over het niet reageren op de oproepingen van de autoriteit;

Het kan interessant zijn om te weten dat een persoon die opgenomen is in de gemeenschappelijke gegevensbank T.E.R., niet op zijn of haar afspraken opdaagt of niet reageert op de aanmaningen van de rechters.

v. de vervoermiddelen;

De vervoermiddelen worden ook geregistreerd.

Het gaat om de vervoermiddelen die de betrokken persoon gebruikt. Bijgevolg beperkt deze categorie zich niet tot het vervoermiddel waarvan hij de eigenaar is, maar kan het ook gaan om de wagen van de moeder, van een vriend(in), enz. Het gaat daarentegen niet om een vervoermiddel waarvan de entiteit regelmatig passagier is. Indien de entiteit enkel het openbaar vervoer gebruikt, kan dat element eveneens worden vermeld in de gegevensbank.

Het is voor de basisdiensten en de partnerdiensten van belang dat het soort vervoermiddel gekend is, alsook het merk, de kleur en het inschrijvingsnummer ervan. Met die gegevens kunnen verschillende inlichtingen aan elkaar worden gelinkt. Indien een vervoermiddel bijvoorbeeld wordt gezien en het nummer ervan wordt opgemerkt bij verdachte handelingen in de buurt van een luchthaven, een station, een ambassade of een enig ander zenuwpunt in België, moet men kunnen controleren of het voertuig in kwestie een voertuig is dat wordt gebruikt door een entiteit die in de gegevensbank is geregistreerd. In geval van overeenkomst tussen de opgemerkte plaat en een in de gegevensbank geregistreerde plaat, is het vanzelfsprekend dat de informatie over de verdachte handelingen een heel ander gewicht krijgt, met onderzoeken die gericht kunnen zijn op de betrokken entiteit en met passende beschermingsmaatregelen voor de plaatsen die betrokken zijn bij de verdachte handelingen. In het voorgaande voorbeeld vertrok men van het principe dat het voertuig werd gezien op het tijdstip van de verdachte handelingen, maar er kan een vergelijkbare situatie worden aangehaald waarin de kentekenplaat wordt gedetecteerd door een ANPR-systeem dat in de buurt van de plaats van de verdachte handelingen of zelfs een beetje verderop is opgesteld, en daarna in de gemeenschappelijke gegevensbank wordt opgezocht. Het is daarnaast belangrijk om te weten of de entiteit regelmatig verschillende vervoermiddelen of huurvoertuigen gebruikt om samen na te denken over de reden voor die veranderingen of voor het gebruik van huurvoertuigen.

B. Entités personnes morales

Les personnes morales ayant des rapports avec une personne physique enregistrée dans la banque de données peuvent aussi être traitées dans cette banque de données, après concertation au sein de la TFL. Il ne s'agit pas de vouloir multiplier le nombre de personnes morales enregistrées mais d'enregistrer celles qui ont un lien avec des personnes physiques.

En effet, il arrive que de personnes physiques utilisent les structures d'une société ou d'une association pour arriver à leurs fins. On peut évoquer l'exemple d'une société créée en vue de collecter des fonds dont la finalité détournée sera le financement d'actions de terrorisme. On peut dans le même ordre d'idée avoir besoin d'enregistrer une société dont le but est le recrutement d'extrémismes en les attirant par des stages au cours desquels sont enseignées des méthodes de combat armé. Il peut aussi s'avérer nécessaire de traiter les données d'une personne morale lorsque celle-ci est la seule source identifiée dans le contexte du terrorisme ou de l'extrémisme pouvant mener au terrorisme. Dans ce cas, c'est d'abord la personne morale qui apparaît au moment de la détection d'intentions de terrorisme. Les personnes physiques se cachent derrière cette structure de sorte qu'il n'est pas possible de les identifier directement. Il faut pourtant partager cette donnée dans la banque de données commune afin que la personne morale reste sur les radars et que les services contribuent à compléter l'information pour permettre de lier des personnes physiques à cette organisation. Le but sera ensuite de déterminer le rôle de chaque personne et la nature de ses actions. La personne physique n'est elle-même enregistrée dans la banque de données que si les données sont suffisantes pour que l'analyse démontre qu'elle fait partie de l'une des catégories de personnes dont les données peuvent être traitées.

Ainsi, outre les données précitées, les données relatives à une personne morale suivantes seront également traitées dans la banque de données commune T.E.R.:

- a) la dénomination et s'il échet l'abréviation;
- b) le pays d'origine;
- c) l'adresse du siège;
- d) le type d'activités du groupement;

Pour les personnes morales, les données traitées concernent la dénomination, le pays d'origine, car il se peut qu'il ne soit pas systématiquement la Belgique, l'adresse de son siège et son activité principale telle qu'elle a été déclarée.

B. Entiteiten die rechtspersoon zijn

De rechtspersonen die banden hebben met een natuurlijke persoon die in de gegevensbank is geregistreerd, kunnen na overleg in de LTF ook in die gegevensbank worden verwerkt. Het is niet de bedoeling om grote aantallen rechtspersonen te registreren, maar om degenen die een band hebben met natuurlijke personen te registreren.

Het gebeurt immers dat natuurlijke personen de structuren van een vennootschap of een vereniging gebruiken om hun doeleinden te bereiken. Bijvoorbeeld een vennootschap die werd opgericht voor geldinzameling met als verborgen finaliteit de financiering van terreurdaden. In diezelfde zin kan er een behoefte zijn om een vennootschap te registreren, die bedoeld is om extremisten te ronselen door hen aan te trekken met stages in de loop waarvan zij gewapende gevechtsmethoden leren. Het kan ook nodig zijn om de gegevens van een rechtspersoon te verwerken wanneer die de enige bron is die geïdentificeerd is in de context van terrorisme of extremisme die kan leiden tot terrorisme. In dat geval is het eerst de rechtspersoon die opduikt wanneer terroristische bedoelingen worden ontdekt. De natuurlijke personen verbergen zich achter die structuur zodat het niet mogelijk is om hen rechtstreeks te identificeren. Dat gegeven moet echter worden gedeeld in de gemeenschappelijke gegevensbank, zodat de rechtspersoon op de radar blijft en zodat de diensten de inlichtingen aanvullen om natuurlijke personen aan die organisatie te kunnen linken. Het is vervolgens de bedoeling om te bepalen welke rol elke persoon speelt en wat de aard van zijn handelingen is. De natuurlijke persoon zelf wordt enkel in de gegevensbank geregistreerd wanneer er voldoende gegevens zijn om aan te tonen dat hij deel uitmaakt van een van de categorieën van personen wier gegevens kunnen worden verwerkt.

Naast de bovengenoemde gegevens worden dus ook de volgende gegevens betreffende een rechtspersoon in de gemeenschappelijke gegevensbank T.E.R. verwerkt:

- a) de naam en, indien van toepassing, de afkorting;
- b) het land van oorsprong;
- c) het adres van de zetel;
- d) de aard van de activiteiten van de groepering;

De gegevens die verwerkt worden voor de rechtspersonen, zijn de benaming, het land van oorsprong – want het kan dat het niet systematisch België is –, het adres van de zetel en de hoofdactiviteit zoals die werd aangegeven.

e) les éléments liés à sa localisation;

Outre l'adresse du siège social, il est important de connaître les autres lieux d'activité de la personne morale. Ce sont les adresses en Belgique qui vont permettre aux services d'assurer un suivi ou d'envisager les actions nécessaires. D'autre part, ces localisations permettent de faire circuler les informations vers les services territorialement compétents et, le cas échéant, activer plus dynamiquement l'effort de recherche d'informations.

f) les moyens de transport;

Comme expliqué ci-dessus pour les moyens de transport de la personne concernée, cette dernière pourrait utiliser des moyens de transport dont elle n'est pas propriétaire. Ainsi elle pourrait utiliser le véhicule de la personne morale. C'est pourquoi cette donnée doit également être enregistrée.

g) communication: numéro de téléphone, réseaux sociaux, etc.;

Ces données sont enregistrées pour les mêmes raisons que celles exposées plus haut au sujet des moyens de communication des personnes physiques.

h) les personnes autorisées à administrer et à représenter la société;

Ces informations sont nécessaires pour déterminer la fonction de la personne concernée. C'est un élément essentiel dans l'évaluation de la menace car il faut savoir si une entité enregistrée dans la banque de données a le pouvoir d'orienter la société vers la réalisation de ses objectifs ou si la fonction occupée ne le permet pas.

i) Situation juridique: faillite, etc.;

La situation juridique de la personne morale permet de connaître l'objectif initial, déterminé au moment de sa création.

Ce paramètre permet lui aussi d'analyser le risque puisqu'il est possible que l'intention initiale se soit traduite différemment dans les faits ou qu'il y ait eu une déviation complète des objectifs et une finalité émergente de commettre des actes terroristes, après, par exemple, une tendance progressive vers différentes formes d'extrémisme.

e) elementen met betrekking tot de locatie;

Naast het adres van de maatschappelijke zetel is het belangrijk om te weten of de rechtspersoon activiteiten uitoefent op andere plaatsen. Dat zijn adressen in België waardoor de diensten voor een opvolging kunnen zorgen of de vereiste acties kunnen overwegen. Daarnaast kan door die locaties informatie worden doorgegeven aan de territoriaal bevoegde diensten en kunnen, in voorkomend geval, de inspanningen op het stuk van informatiegaring dynamischer worden gestimuleerd.

f) de vervoermiddelen;

Zoals hierboven reeds toegelicht voor de vervoermiddelen van de betrokken persoon, kan deze laatste vervoermiddelen gebruiken waarvan hij niet de eigenaar is. Zo kan hij het voertuig van de rechtspersoon gebruiken. Daarom moet die informatie ook worden geregistreerd.

g) communicatie: telefoonnummer, sociale media, enz.;

Die gegevens worden geregistreerd om dezelfde redenen als degene die hierboven werden toegelicht met betrekking tot de communicatiemiddelen van de natuurlijke personen.

h) de personen die bevoegd zijn om de vennootschap te beheren en te vertegenwoordigen;

Die informatie is noodzakelijk om de functie van de betrokken persoon te bepalen. Het is een essentieel element bij de dreigingsevaluatie, want men moet weten of een entiteit die in de gegevensbank is geregistreerd, de mogelijkheid heeft om de vennootschap naar haar hand te zetten voor de verwezenlijking van haar doeleinden of dat de beklede functie dat niet toelaat.

i) rechtstoestand: failliet, enz.;

Door de rechtstoestand van de rechtspersoon is het mogelijk om de oorspronkelijke doelstelling te kennen, die werd bepaald op het tijdstip van zijn oprichting.

Met die parameter kan het risico worden geanalyseerd, want het is mogelijk dat de oorspronkelijke bedoeling in feite anders wordt ingevuld of dat er volledig van de doelstellingen is afgeweken en er een plan om terreurdaden te plegen tevoorschijn komt na, bijvoorbeeld, een progressieve tendens naar verschillende vormen van extremisme.

C. Entités qui sont des associations de fait

Suite à l'avis du Comité R du 13 juillet 2023 (§ 22), il est précisé quelles données à caractère personnel peuvent être enregistrées dans la banque de données commune T.E.R. concernant les associations de fait. Il s'agit des mêmes données que pour les personnes morales à l'exception de la situation juridique dans la mesure où les associations de fait n'ont pas de personnalité juridique.

II. — LES DONNÉES ADMINISTRATIVES, JUDICIAIRES, DE POLICE JUDICIAIRE, DE POLICE ADMINISTRATIVE ET LES INFORMATIONS RELATIVES AUX ENTITÉS ENREGISTRÉES

En ce qui concerne le deuxième type de données à caractère personnel traitées dans la banque de données commune T.E.R., il n'est pas possible d'énumérer ici toutes les données visées à l'article 6, § 2, 2°, mais différents exemples permettent de comprendre les données concernées. Premièrement, les données traitées sont les données judiciaires relatives à l'entité: la détention préventive; la détention préventive sous surveillance électronique; la remise en liberté sous conditions; l'existence d'un mandat d'arrêt international; l'existence d'un mandat d'arrêt européen; la décision des juridictions d'instruction statuant sur le fond (l'internement et la suspension du prononcé); la fixation d'une affaire pénale devant le tribunal correctionnel, la cour d'appel et la cour d'assises et la condamnation/l'acquittement.

Le Ministère public n'enregistrera dans la banque de données commune T.E.R. que les données judiciaires précitées. Le Collège des procureurs généraux prendra une circulaire nationale avec des directives contraignantes à ce sujet.

Autre exemple, dans le cadre du suivi d'entités pour lesquelles il existe un mandat des autorités judiciaires, les données judiciaires telles que le type de mandat de suivi, le début et la fin du mandat ou la maison de justice compétente pourront également être enregistrées par le service compétent dans la banque de données commune T.E.R.

Deuxièmement, des données administratives seront également traitées. Il s'agit par exemple de la catégorie de personnes à laquelle l'entité appartient (FTF, propagandiste...), du port ou de la détention autorisée d'une

C. Entiteiten die feitelijke verenigingen zijn

Ingevolge het advies van Comité I van 13 juli 2023 (§ 22) wordt verduidelijkt welke persoonsgegevens in de gemeenschappelijke gegevensbank T.E.R. kunnen worden opgenomen aangaande feitelijke verenigingen. Het zijn dezelfde gegevens als voor rechtspersonen, met uitzondering van de rechtstoestand, aangezien feitelijke verenigingen geen rechtspersoonlijkheid hebben.

II. — DE ADMINISTRATIEVE GEGEVENS, DE GERECHTELIJKE GEGEVENS, DE GEGEVENS VAN GERECHTELIJKE POLITIE, DE GEGEVENS VAN BESTUURLIJKE POLITIE EN DE INFORMATIE BETREFFENDE DE GEREГИSTREERDE ENTITEITEN

Met betrekking tot het tweede type van persoonsgegevens dat in de gemeenschappelijke gegevensbank T.E.R. wordt verwerkt, is het niet mogelijk om hier alle gegevens op te lijsten die worden bedoeld in artikel 6, § 2, 2°, maar de betrokken gegevens kunnen worden begrepen aan de hand van verschillende voorbeelden. Eerst en vooral zijn de verwerkte gerechtelijke gegevens met betrekking tot de entiteit: de voorlopige hechtenis; de voorlopige hechtenis onder elektronisch toezicht; de vrijlating onder voorwaarden; het bestaan van een internationaal aanhoudingsbevel; het bestaan van een Europees aanhoudingsbevel; de beslissing van de onderzoeksgerechten zetelend ten gronde (de internering en de opschorting van de uitspraak); de vaststelling van een strafzaak voor de correctionele rechtbank, het hof van beroep of het hof van assisen en de veroordeling/vrijpraak.

Het openbaar ministerie neemt enkel de voorgaande gerechtelijke gegevens op in de gemeenschappelijke gegevensbank T.E.R. Het College van procureurs-generaal zal een nationale omzendbrief uitvaardigen met dwingende richtlijnen daaromtrent.

In het kader van het toezicht op entiteiten waarvoor een mandaat van de gerechtelijke overheden bestaat, kunnen bijvoorbeeld ook gerechtelijke gegevens zoals het soort controleopdracht, het begin en het einde van het mandaat of het bevoegde Justitiehuis in de gemeenschappelijke gegevensbank T.E.R. worden door de bevoegd dienst geregistreerd.

In de tweede plaats, zullen ook administratieve gegevens worden verwerkt. Dit gaat bijvoorbeeld om de categorie van personen waartoe de entiteit behoort (FTF, haatpropagandist...), om het vergunde vuurwapenbezit

arme à feu, du niveau de menace que représente l'entité, des données relatives à la détention dans un établissement pénitentiaire ou encore des données relatives aux voyages effectués à l'étranger. Enfin, il peut s'agir de données émanant de l'office des étrangers en ce qui concerne la situation de la personne sur le territoire (séjour, établissement...) et des éventuelles procédures en cours dans ce cadre.

Troisièmement, seront également traitées dans la banque de données commune T.E.R., des données de police judiciaire telles que les antécédents en matière de terrorisme, l'existence d'un signalement national ou international sur base d'un mandat d'arrêt (européen ou international), etc. ainsi que les données de police administrative comme l'appartenance à un groupement suspectée de terrorisme, etc. et les données de renseignements (médias sociaux, etc.);

Les données de police judiciaire sont les données traitées par les services de police qui sont relatives aux infractions commises, c'est-à-dire les délits et les crimes et les données relatives à ces infractions (la qualification, la date, la localisation, le mode opératoire...). Ces données ont également trait aux enquêtes menées, elles sont traitées dans la banque de données conformément aux instructions des autorités judiciaires. Citons aussi les mesures de police judiciaire qui font partie de cette catégorie de données: arrêter; entendre avec privation de liberté; contacter immédiatement le service de police ou le magistrat responsable...

Suite à l'avis du C.O.C. du 20 juin 2023 au sujet de l'article 6, § 2, 2°, il convient de préciser que tous les types d'informations et données à caractère personnel policières (non classifiées) peuvent être enregistrées dans la banque de données commune T.E.R., mais elles le seront parfois en partie, notamment lorsqu'elles n'auront pas encore été validées.

Les données de police administrative sont par exemple les données d'organisation ou de participation à certains événements. Il est utile de rappeler que les données doivent être adéquates, pertinentes et non excessives au regard des finalités définies dans la loi en ce qui concerne la banque de données commune. On ne vise donc pas la simple participation à une marché hebdomadaire. Il faut que cette participation présente un lien avec la prévention et le suivi du terrorisme et de l'extrémisme lorsqu'il peut mener au terrorisme. Le même raisonnement vaut dans le cas de l'organisation d'un événement.

of de vergunde vuurwapendracht, het dreigingsniveau van de entiteit, de gegevens met betrekking tot de detentie in een penitentiare inrichting of gegevens met betrekking tot reizen naar het buitenland. Tot slot kan het gaan om gegevens van de Dienst Vreemdelingenzaken met betrekking tot de situatie van de persoon op het grondgebied (verblijf, vestiging...) en mogelijke lopende procedures in kader daarvan.

In de derde plaats, zullen ook gegevens van gerechtelijke politie in de gemeenschappelijke gegevensbank T.E.R. worden verwerkt zoals de antecedenten op het vlak van terrorisme, het bestaan van een nationale of internationale seining op basis van een (Europees of internationaal) aanhoudingsmandaat, enz. alsook gegevens van bestuurlijke politie, zoals lidmaatschap van een van terrorisme verdachte groepering, enz., en inlichtingengegevens (sociale media, enz.);

De gegevens van gerechtelijke politie zijn gegevens die door de politie worden verwerkt met betrekking tot de gepleegde misdrijven, dat wil zeggen de wanbedrijven en misdaden en de gegevens met betrekking tot die misdrijven (de kwalificatie, de datum, de plaats, de *modus operandi*...). Die gegevens gaan eveneens over de gevoerde onderzoeken; zij worden verwerkt in de gegevensbank overeenkomstig de instructies van de gerechtelijke overheden. Ook de maatregelen van gerechtelijke politie maken deel uit van die gegevenscategorie: aanhoudingen; verhoor met vrijheidsbeneming; onmiddellijk contacteren van de politiedienst of de verantwoordelijke magistraat...

Ingevolge het advies van 20 juni 2023 van het COC inzake artikel 6, § 2, 2°, moet er worden verduidelijkt dat alle mogelijke politionele (niet-geclassificeerde) informatie en persoonsgegevens kunnen worden opgenomen in de gemeenschappelijke gegevensbank T.E.R., maar dat dat soms maar gedeeltelijk het geval zal zijn, met name wanneer ze nog niet zijn gevalideerd.

De gegevens van de bestuurlijke politie zijn bijvoorbeeld gegevens over het organiseren of bijwonen van bepaalde evenementen. Het is nuttig om eraan te herinneren dat de gegevens toereikend, ter zake dienend en niet overmatig moeten zijn in verhouding tot de in de wet bepaalde doelmatigheden met betrekking tot de gemeenschappelijke gegevensbank. De loutere deelname aan een wekelijkse markt wordt dus niet beoogd. Die deelname moet een link hebben met de preventie en opvolging van terrorisme en van extremisme wanneer dat kan leiden tot terrorisme. Dezelfde redenering wordt gevolgd in het geval van de organisatie van een evenement.

III. — LES DONNÉES OU CODES D'IDENTIFICATION DES PERSONNES OU DES SERVICES AYANT ACCÈS À LA BANQUE DE DONNÉES COMMUNE T.E.R.

La troisième et dernière catégorie de données qui seront traitées dans la banque de données commune T.E.R. sont les données ou codes d'identification des accès à la banque de données commune. Les données à caractère personnel ou, en ce qui concerne les membres des services de renseignements et de sécurité, les codes d'identification des utilisateurs sont également enregistrés (logging) dans la banque de données commune, ce qui est non seulement intéressant sur le plan opérationnel (savoir qui a ajouté telle donnée permet de renforcer la collaboration entre les différents partenaires) mais aussi sur le plan de la sécurité (qui a modifié, supprimé, quand, ...).

Le type de données à caractère personnel est désormais déterminé dans la loi plutôt que dans l'arrêté royal afin de donner une base légale forte en matière de traitements de données à caractère personnel.

Le présent projet exclut cependant les renseignements classifiés provenant par exemple, des services de renseignement et de sécurité. La banque de données commune T.E.R. est une banque de données qui est mise à la disposition de plusieurs partenaires, qui ne sont pas habitués à traiter des informations classifiées et elle ne répond pas aux normes imposées pour traiter des données classifiées in extenso. C'est pourquoi les données classifiées ne sont pas traitées dans la banque de données commune T.E.R.

Il faut cependant parvenir à mettre en commun un maximum d'informations pour atteindre l'objectif poursuivi tout en veillant aussi à ne pas mettre gravement en péril une personne ou une enquête importante.

Il est clair que la banque de données commune T.E.R. exige une collaboration entre les partenaires basée sur le respect mutuel, la compréhension et la confiance.

Dans cette optique, les informations classifiées ne pourront certainement pas pour autant être complètement ignorées car elles peuvent être pertinentes à prendre en compte dans l'évaluation de la menace de l'entité concernée. Ces informations seront donc d'une part traitées in extenso dans d'autres systèmes mais elles seront partagées dans le cadre des task forces locales où les représentants des services à l'origine de ces

III. — DE IDENTIFICATIEGEGEVENS OF DE IDENTIFICATIECODES VAN DE PERSONEN OF DE DIENSTEN DIE TOEGANG HEBBEN TOT DE GEMEENSCHAPPELIJKE GEGEVENS BANK T.E.R.

De derde en laatste categorie van gegevens die in de gemeenschappelijke gegevensbank T.E.R. zullen worden verwerkt, zijn de identificatiegegevens of de identificatiecodes van de toegangen tot de gemeenschappelijke gegevensbank. De persoonsgegevens of – wat de leden van de inlichtingen- en veiligheidsdiensten betreft – de identificatiecodes van de gebruikers worden tevens geregistreerd (oplijsting, logging) in de gemeenschappelijke gegevensbank. Dit is niet alleen interessant op operationeel vlak (weten wie een bepaald gegeven toegevoegd heeft, maakt het mogelijk de samenwerking tussen de verschillende partners te versterken) maar ook op het vlak van de beveiliging (wie heeft gewijzigd, uitgewist, wanneer, ...).

Het type van persoonsgegevens wordt voortaan veeleer in de wet bepaald dan in het koninklijk besluit teneinde te voorzien in een sterke wettelijke grondslag op het gebied van verwerkingen van persoonsgegevens.

Dit ontwerp sluit echter de geclassificeerde inlichtingen uit, bijvoorbeeld afkomstig van de inlichtingen- en veiligheidsdiensten. De gemeenschappelijke gegevensbank T.E.R. is een gegevensbank die ter beschikking wordt gesteld van verschillende partners die het niet gewoon zijn geclassificeerde informatie te verwerken, en voldoet niet aan de opgelegde normen voor de verwerking van geclassificeerde informatie in extenso. Daarom worden er geen geclassificeerde gegevens verwerkt in de gemeenschappelijke gegevensbank T.E.R.

Om het nagestreefde doel te bereiken, moet men echter komen tot een gemeenschappelijke terbeschikkingstelling van een maximum aan informatie terwijl er tegelijkertijd over gewaakt moet worden dat een belangrijk persoon of, onderzoek, niet ernstig in gevaar wordt gebracht.

Het is duidelijk dat de gemeenschappelijke gegevensbank T.E.R. een samenwerking tussen de partners vereist die gebaseerd is op wederzijds respect, begrip en vertrouwen.

In dat opzicht kan de geclassificeerde informatie zeker niet volledig worden genegeerd daar ze relevant kan zijn om rekening mee te houden in de beoordeling van de dreiging van de betrokken entiteit. Deze informatie zal enerzijds dus in andere systemen in extenso verwerkt worden, maar ze zal gedeeld worden in het kader van de lokale task forces waarin de vertegenwoordigers van de diensten die aan de oorsprong van deze informatie

informations sont présents. Il est renvoyé au chapitre 3 du présent projet pour plus de détails sur ce point.

De plus, il faut également rappeler que la finalité de la banque de données commune T.E.R. est notamment d'assurer un suivi des entités. Dans l'exemple extrême où toute l'information d'une entité est classifiée, un suivi sera quand même assuré, mais d'une autre manière. Les services concernés recevront les informations classifiées par les canaux de communication appropriés. Un échange est également instauré au sein de "la Task Force locale". Lorsque la majorité des informations est classifiée, seules les données d'identification (non classifiées) de l'entité seront d'autre part mentionnées dans la banque de données commune, mais avec quand même une indication quant à l'existence d'informations classifiées.

Art. 7

À titre préliminaire, il faut préciser que dans son avis du 20 juin 2023, le C.O.C. demande à l'auteur du projet de réfléchir et de procéder au moins à un examen critique du système d'archivage envisagé, qui fait double emploi avec ce qui est prévu dans la loi sur la fonction de police. Or, la banque de données commune T.E.R. n'est pas une banque de données de la police. On ne peut dès lors pas lui appliquer d'office les dispositions de la loi sur la fonction de police. C'est d'ailleurs une des raisons pour laquelle les dispositions relatives à la banque de données commune qui figurent dans la loi sur la fonction de police sont reprises dans une loi autonome et que des règles propres à cette banque de données sont prévues.

L'article 44/11/3bis, §§ 5 et 7, de la loi sur la fonction de police est repris à l'article 7, §§ 1 et 3. Le projet en simplifie toutefois l'écriture, notamment pour bien faire comprendre le moment où l'archivage intervient. Notons que dans l'article 7, les termes "suppression et archivage" ont été préférés à "effacement et conservation".

Le paragraphe 1^{er} prévoit que les données à caractère personnel conservées dans la banque de données commune sont archivées dès que les finalités de la banque de données commune ne sont plus rencontrées et, au maximum 30 ans après le dernier enregistrement d'une donnée ou information dans la fiche de renseignement de l'entité validée. Il est tenu compte ici de la remarque de l'Autorité de protection des données (cf. Avis n° 97/2023 du 16 juin 2023, § 115). Une exception est toutefois faite concernant les données à caractère personnel relatives à des mineurs qui sont conservées au

liggen, aanwezig zijn. Er wordt verwezen naar hoofdstuk 3 van dit ontwerp voor meer details over dit punt.

Bovendien dient men er eveneens aan te herinneren dat het doeleinde van de gemeenschappelijke gegevensbank T.E.R. onder meer bestaat uit het verzekeren van de opvolging van de entiteiten. In het extreme voorbeeld waar alle informatie over een entiteit geëncrypteerd is, zal een opvolging toch mogelijk zijn, maar op een andere manier. De betrokken diensten zullen geëncrypteerde informatie via de passende communicatiekanalen ontvangen. Daarnaast wordt ook informatie uitgewisseld binnen de "Local Task Force". Wanneer het overgrote deel van de informatie geëncrypteerd is, worden anderzijds enkel de identificatiegegevens (niet-geëncrypteerd) van de entiteit vermeld in de gemeenschappelijke gegevensbank, doch met een indicatie over het bestaan van geëncrypteerde informatie.

Art. 7

Ter inleiding moet worden verduidelijkt dat het COC in het advies van 20 juni 2023 de auteur van het ontwerp verzoekt zich te beraden en minstens een kritische toetsing te doen van het beoogde archiveringssysteem, dat overlapt met dat waarin in de wet op het politieambt is voorzien. De gemeenschappelijke gegevensbank T.E.R. behoort echter niet toe aan de politie. Dat betekent dus dat de bepalingen van de wet op het politieambt er niet standaard van op toepassing zijn. Dat is trouwens een van de redenen waarom de bepalingen met betrekking tot de gemeenschappelijke gegevensbank uit de wet op het politieambt worden overgezet in een autonome wet en dat er voorzien is in regels die specifiek gelden voor deze gegevensbank.

Artikel 44/11/3bis, §§ 5 en 7, van de wet op het politieambt wordt hernomen in artikel 7, §§ 1 en 3. Het ontwerp vereenvoudigt echter de formulering ervan, om duidelijk te maken wanneer de archivering gebeurt. Opgemerkt zij dat in artikel 7 de voorkeur is gegeven aan de termen "verwijdering en archivering" boven "uitwissing en bewaring".

Paragraaf 1 bepaalt dat de in de gemeenschappelijke gegevensbank opgeslagen persoonsgegevens worden gearhiveerd vanaf het ogenblik dat de doeleinden van de gemeenschappelijke gegevensbank niet meer worden bereikt en maximaal 30 jaar na de laatste opname van een gegeven of van informatie in de inlichtingenfiche van de gevalideerde entiteit. Hier wordt rekening gehouden met de opmerking van de Gegevensbeschermingsautoriteit (zie advies nr. 97/2023 van 16 juni 2023, § 115). Een uitzondering wordt gemaakt voor persoonsgegevens van minderjarigen, die maximaal 15 jaar na de laatste

maximum 15 ans après le dernier enregistrement d'une donnée ou information. Cette différence de conservation des données se justifie en raison de l'approche plus protectrice souhaitée à l'égard des mineurs.

Il s'agit, au paragraphe 1^{er}, des principes de bonne gestion et du suivi régulier de la qualité des données à caractère personnel et des informations pour que la banque de données commune soit "dynamique" et ne contienne pas de données inutiles.

Ce paragraphe prévoit également que l'examen des données à caractère personnel et des informations afin de vérifier si celles-ci répondent toujours à l'une des finalités poursuivies par la création de la banque de données commune, a lieu tous les cinq ans sans attendre l'archivage au terme du délai maximal prévu. Cet examen doit se lire comme une garantie supplémentaire qui se rajoute à l'obligation de l'OCAM de réaliser des évaluations de la menace en continu (et actualiser cette évaluation au minimum deux fois par ans). À noter que ce délai est porté à trois ans en ce qui concerne l'examen des données à caractère personnel et des informations relatives à des mineurs pour les raisons évoquées ci-avant. Un délai de cinq ans est prévu par parallélisme avec le délai prévu par la loi du 10 juillet 2006 relative à l'analyse de la menace.

Dans son avis du 13 juillet 2023, le Comité R recommande de modifier le système de calcul de la durée de conservation des données car il estime qu'il a pour effet de prolonger indéfiniment la conservation des données (§ 8). Or, comme indiqué ci-avant, le dispositif de l'article 7 stipule que le délai maximum de conservation des données est de 30 ans. Il s'agit donc d'un maximum absolu. Dans la mesure où une finalité ne serait plus rencontrée, les données visées doivent être archivées immédiatement sans attendre la fin du délai maximum de 30 ans. Le dispositif prévoit le cas spécifique de données qui ne sont plus "utilisées" pendant une certaine période. Pour éviter que des données à caractère personnel soient simplement "oubliées" plutôt que supprimées ou archivées avant l'expiration du délai de 30 ans, l'avant-projet de loi impose un contrôle régulier de la pertinence de conserver ces données qui n'ont plus fait l'objet d'un enregistrement de données depuis un certain temps. Il appartient en outre aux autorités de contrôle de vérifier le respect des délais.

Le Comité R estime également que l'obligation pour le responsable opérationnel d'examiner le "lien direct" entre les données à caractère personnel et les finalités de l'article 5, alinéa 2, ne se substitue pas aux obligations qui découlent des articles 140 et 141 de la loi

verwerking van een gegeven of van informatie worden bewaard. Dat verschil in gegevensbewaring wordt verantwoord door de gewenste beschermendere aanpak jegens minderjarigen.

In paragraaf 1 gaat het om de principes van goed beheer en van regelmatige opvolging van de kwaliteit van de persoonsgegevens en van de informatie opdat de gemeenschappelijke gegevensbank "dynamisch" zou zijn en geen overbodige gegevens bevat.

Vornoemde paragraaf voorziet ook dat de persoonsgegevens en de informatie om de vijf jaar worden onderzocht om na te gaan of deze nog steeds beantwoorden aan een van de doeleinden die worden nagestreefd door de oprichting van de gemeenschappelijke gegevensbank zonder de archivering op het einde van de maximumtermijn waarin is voorzien af te wachten. Dat onderzoek moet worden gelezen als een extra waarborg boven op de verplichting van het OCAD om de dreiging voortdurend te evalueren (en ten minste tweemaal per jaar bij te werken). Deze termijn wordt verlengd tot drie jaar voor het onderzoek van persoonsgegevens en informatie betreffende minderjarigen om de hierboven aangehaalde redenen. Er is voorzien in een periode van vijf jaar, parallel met de periode voorzien in de wet van 10 juli 2006 betreffende de analyse van de dreiging.

In het advies van 13 juli 2023 beveelt het Comité I aan om het systeem voor de berekening van de bewaaringstermijn van de gegevens te wijzigen, want het oordeelt dat het als gevolg heeft dat de bewaring van de gegevens voor onbepaalde tijd wordt verlengd (§ 8). Zoals hierboven vermeld bepaalt artikel 7 dat de maximale bewaaringstermijn 30 jaar bedraagt. Het gaat dan ook om een absoluut maximum. Voor zover een doeleinde niet meer zou worden verwezenlijkt, moeten de beoogde gegevens onmiddellijk worden gearchiveerd zonder het einde van de maximumtermijn van dertig jaar af te wachten. De bepaling voorziet in het specifieke geval van gegevens die niet meer worden "gebruikt" gedurende een bepaalde periode. Om te voorkomen dat persoonsgegevens simpelweg zouden worden "vergeten" in plaats van verwijderd of gearchiveerd na het verstrijken van de termijn van 30 jaar, legt het voorontwerp van wet een regelmatige controle op van de relevantie van de bewaring van die gegevens die gedurende een bepaalde tijd niet meer zijn geregistreerd. Het is bovendien aan de toezichthoudende overheden om de inachtneming van de termijnen te controleren.

Het Comité I oordeelt eveneens dat de verplichting van de operationeel verantwoordelijke om het "rechtstreekse verband" tussen de persoonsgegevens en de doeleinden van artikel 5, § 2, te onderzoeken, niet in de plaats komt van de verplichtingen die voortvloeien uit de

relative à la protection des données (qui s'appliquent en continu) et ne permet pas, à elle seule, de remplir ces obligations prévues par ladite loi (§ 9). Outre les explications évoquées ci-avant, comme le prévoit l'avant-projet de loi, il est effectivement prévu que les articles 140 et 141 s'appliquent en continu. Cependant, l'avant-projet entend renforcer les obligations en matière de conservation des données qui ne sont manifestement plus traitées depuis un certain temps. Le fait de ne pas traiter des données à caractère personnel durant une certaine période ne peut signifier en soi que la finalité pour laquelle les données ont été enregistrées n'existent plus mais l'auteur du projet entend imposer un contrôle formel de cette finalité dans ce cas précis. Les données en cours de traitement ou qui font l'objet d'un traitement régulier impliquent un contrôle actif du lien avec la finalité de leur enregistrement.

La remarque du Comité R suggère donc la suppression de la disposition qui impose un contrôle périodique de certaines données. Nous n'estimons pas qu'une telle suppression soit de nature à renforcer la protection des personnes au regard du traitement de leurs données à caractère personnel. Le simple fait qu'une personne enregistrée dans la banque de données commune ne fasse plus parler d'elle durant un certain laps de temps n'a pas pour conséquence directe de rompre le lien avec la finalité pour laquelle les données de cette personne ont été enregistrées dans la banque de données. Imposer un contrôle constant, et donc humain, dans ce cas de figure paraît excessif et peu raisonnable en termes de moyen. Le caractère raisonnable de la mise en œuvre des principes de traitement des données à caractère personnel n'est pas mise en doute par l'auteur du projet. Il entend néanmoins aider le responsable du traitement à respecter ses obligations en fixant des critères minimaux à appliquer pour un traitement correct des données à caractère personnel dans certains cas de figure. L'obligation formelle d'examiner périodiquement la finalité de la données enregistrée qui ne fait plus l'objet d'un enregistrement de données depuis un laps de temps fait partie de ces cas.

Ensuite, le Comité R ne comprend pas comment l'auteur du projet justifie qu'une évaluation de la menace des entités ait lieu deux fois par an au minimum par l'OCAM (art. 27), alors que le responsable opérationnel n'est obligé d'examiner "le lien direct" entre les données et les finalités de l'article 5, alinéa 2 que tous les 5 ans. Il indique que l'analyse de la menace doit être effectuée sur la base de données qui répondent aux normes des articles 140 et 141 de la loi relative à la protection des données et qu'avant d'analyser la menace, le responsable

articles 140 et 141 van de wet tot bescherming van de persoonlijke levenssfeer (die voortdurend van toepassing zijn) en op zich niet voldoet die verplichtingen zoals bepaald door die wet (§ 9). Naast de hiervoor vermelde uitleg zoals bepaald in het voorontwerp van wet wordt er daadwerkelijk bepaald dat de artikelen 140 en 141 voortdurend van toepassing zijn. Het voorontwerp wil evenwel de verplichtingen versterken op het stuk van de bewaring van de gegevens die kennelijk al enige tijd niet meer zijn verwerkt. Het feit dat de persoonsgegevens niet meer worden verwerkt gedurende een bepaalde periode, kan op zich niet betekenen dat het doeleinde waarvoor de gegevens zijn geregistreerd, niet meer bestaat, maar de auteur van dit ontwerp wil in dat specifieke geval een formele controle van dat doeleinde opleggen. De gegevens die in verwerking zijn of die regelmatig worden verwerkt, vergen een actieve controle van de band met het doeleinde van hun registratie.

De opmerking van het Comité I suggereert dus de schrapping van de bepaling die een periodieke controle van bepaalde gegevens oplegt. Wij vinden niet dat een dergelijke schrapping van dien aard is dat de bescherming van de personen ten aanzien van de verwerking van hun persoonsgegevens wordt versterkt. Het loutere feit dat er gedurende een bepaalde periode niet meer over een in de gemeenschappelijke gegevensbank geregistreerde persoon wordt gesproken, heeft niet tot rechtstreeks gevolg dat de band met het doeleinde waarvoor de gegevens van die persoon werden geregistreerd in de gegevensbank wordt verbroken. Een voortdurende, en dus menselijke, controle opleggen in dat geval lijkt overdreven en niet erg redelijk op het stuk van middelen. Het redelijke karakter van de tenuitvoerlegging van de beginselen inzake de verwerking van persoonsgegevens wordt niet in twijfel getrokken door de auteur van het ontwerp. Het is niettemin de bedoeling de verwerkingsverantwoordelijke te helpen bij het naleven van zijn verplichtingen door de toe te passen minimale criteria voor een correcte verwerking van de persoonsgegevens in bepaalde gevallen vast te leggen. De formele verplichting om periodiek het doeleinde te onderzoeken van de gegevens waarvoor geen gegevens meer geregistreerd werden, maakt deel uit van die gevallen.

Vervolgens begrijpt het Comité I niet hoe de auteur van het ontwerp rechtvaardigt dat het OCAM ten minste twee keer per jaar een dreigingsevaluatie van de entiteiten moet uitvoeren (art. 27), terwijl de operationele verantwoordelijke slechts verplicht is om elke vijf jaar "het rechtstreekse verband" tussen de gegevens en de doeleinden van artikel 5, tweede lid, te onderzoeken. Het vermeldt dat de dreigingsanalyse moet worden uitgevoerd op basis van gegevens die voldoen aan de normen van de artikelen 140 en 141 van de wet gegevensbescherming

du traitement ou son préposé doit s'assurer (entre autres) de la pertinence des données à caractère personnel. Il recommande ainsi que l'évaluation des données personnelles traitées (qui doivent toujours être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées) aient lieu au minimum tous les six mois (§ 9). À ce sujet, l'interprétation donnée par le Comité R ne reflète ni la réalité du texte en projet ni la réalité de terrain: l'ensemble des données contenues dans la banque de données commune est traité d'une manière dynamique. Quant aux traitements des données en tant que telles, il est renvoyé aux commentaires précédents. Concernant l'évaluation de l'OCAM, le même raisonnement peut être *mutatis mutandis* tenu. En effet, il ne peut être mis en doute dans le cadre d'un projet législatif (ou de tout autre projet normatif) que les autorités publiques soumises à des obligations en vertu des dispositions en projet, exécuteront leurs tâches conformément à la volonté de l'auteur. Le fait que les principes applicables au traitement des données à caractère personnel s'applique en tout temps n'est pas remis en cause par le projet du simple fait que l'auteur, partant de ce principe, ne rappelle pas à chacune des règles énoncées que le principe n'est pas remis en cause. Ce serait tout simplement vider les dispositions contenues dans la loi relative à la protection des données de leur substance. Il est donc bien sûr évident que l'OCAM accomplira ses tâches consciencieusement et s'il est compréhensible que le travail d'analyse de l'OCAM n'aboutit pas nécessairement à une modification de son évaluation à chaque instant, l'auteur du projet entend simplement qu'une trace de cette évaluation intervienne au moins tous les 6 mois lorsque l'OCAM n'a pas de raison de modifier son évaluation d'une entité dans un intervalle plus bref.

À noter qu'outre cet examen, le projet de loi prévoit plusieurs mécanismes de contrôle des données contenues dans la banque de données commune T.E.R. Ainsi, premièrement, le responsable opérationnel contrôle la qualité des données traitées au sein de la banque de données commune T.E.R. et s'assure de leur pertinence au regard des finalités (art. 12, al. 2, 1° et 6°). Deuxièmement, les services de base et les services partenaires, qui bénéficient d'un droit de lecture et d'un droit d'écriture sont tenus, respectivement de consulter la banque de données commune T.E.R. et d'y introduire d'office leurs propres données à caractère personnel et les informations pertinentes. Ces données à caractère personnel et informations sont enregistrées dans la banque de données commune, sous leur responsabilité et suivant leurs procédures internes de validation (art. 18, alinéa 1^{er}). Enfin, troisièmement, l'actualisation deux fois par an de l'évaluation de la menace prévue

en dat de verantwoordelijke voor de verwerking of zijn aangestelde, alvorens de dreiging te analyseren, zich (onder andere) moet vergewissen van de relevantie van de persoonsgegevens. Het beveelt dus aan dat de verwerkte persoonsgegevens (die altijd toereikend, ter zake dienend en niet overmatig moeten zijn in verhouding tot de doeleinden waarvoor ze worden verwerkt) ten minste elke zes maanden worden geëvalueerd (§ 9). De interpretatie van het Comité I ter zake weerspiegelt niet de werkelijkheid van de ontworpen tekst noch de werkelijkheid op het terrein: alle gegevens in de gemeenschappelijke gegevensbank worden op dynamische wijze verwerkt. Wat de verwerking van de gegevens als dusdanig betreft, wordt verwezen naar de voorgaande opmerkingen. Dezelfde redenering kan *mutatis mutandis* worden gevolgd voor de evaluatie van het OCAD. Het kan immers niet in twijfel worden getrokken in het kader van een wetgevend ontwerp (of enig ander normatief ontwerp) dat de overheden die krachtens de ontworpen bepalingen aan verplichtingen worden onderworpen, hun taken zullen uitvoeren in overeenstemming met de wil van de auteur. Het feit dat de beginselen die van toepassing zijn op de verwerking van persoonsgegevens altijd van toepassing zijn, wordt niet ter discussie gesteld door het ontwerp door het loutere feit dat de auteur, vertrekkende uit dat beginsel, niet bij elk van de aangehaalde regels herhaalt dat het principe niet ter discussie wordt gesteld. Dat zou de bepalingen in de wet gegevensbescherming gewoonweg uithollen. Het is natuurlijk vanzelfsprekend dat het OCAD zijn taken plichtbewust zal vervullen en hoewel het begrijpelijk is dat het analysewerk van het OCAD niet noodzakelijkerwijs telkens leidt tot een wijziging van zijn evaluatie, is het de loutere bedoeling van de auteur van het ontwerp dat er alle zes maanden een spoor is van die evaluatie, wanneer het OCAD geen reden heeft om zijn evaluatie van een entiteit op kortere termijn te wijzigen.

Er moet worden opgemerkt dat het wetsontwerp, naast dit onderzoek, verschillende mechanismen voorziet om de gegevens in de gemeenschappelijke gegevensbank T.E.R. te controleren. Zo controleert, ten eerste de operationeel verantwoordelijke de kwaliteit van de in de gemeenschappelijke gegevensbank T.E.R. verwerkte gegevens en ziet hij toe op de relevantie ervan in verhouding tot de doeleinden (art. 12, tweede lid, 1° en 6°). Ten tweede, zijn de basisdiensten en de partnerdiensten, die een leesrecht en een schrijfrecht hebben, verplicht respectievelijk de gemeenschappelijke gegevensbank T.E.R. te raadplegen en ambtshalve hun eigen persoonsgegevens en relevante informatie daarin in te voeren. Die persoonsgegevens en informatie worden onder hun verantwoordelijkheid en overeenkomstig hun interne validatieprocedures opgenomen in de gemeenschappelijke gegevensbank (art. 18, eerste lid). Ten derde, ten slotte, garandeert de halfjaarlijkse bijwerking van

à l'article 27 permet également d'assurer un contrôle des données.

La possibilité d'archivage appartient à DRI en tant que responsable technique et au responsable opérationnel. Dans certains cas, l'archivage est automatique au bout de 30 ans et relève de la compétence de DRI. Néanmoins dans d'autres cas, l'archivage peut intervenir au terme d'un examen des données à caractère personnel et des informations afin de vérifier si celles-ci répondent toujours à l'une des finalités poursuivies par la création de la banque de données commune. Ainsi par exemple, dans le cas des mineurs à partir de 12 ans jusqu'à 18 ans inclus enregistrés dans la banque de données commune T.E.R., une attention particulière sera donnée lorsque l'enregistrement du mineur a été lié à la situation de son parent ou assimilé. Dans ce cas, un archivage pourrait intervenir anticipativement. Cet examen et la proposition d'archivage relève de la responsabilité du responsable opérationnel. Dans les faits, les entités sont systématiquement débattues dans le cadre de "la Task Force locale" avant qu'une décision d'archivage soit prise. L'OCAM confirme alors la décision à DRI étant entendu, que l'OCAM doit produire une dernière évaluation qui confirme la décision.

Par dérogation à la règle générale de conservation prévue à l'article 7, § 1^{er}, le paragraphe 2 prévoit une réduction du délai maximum à 6 mois pour les données et informations relatives à une entité en "pré-enquête", c'est-à-dire qui n'entre pas, au moment de son enregistrement dans la banque de données T.E.R., dans les critères pour être considérée comme *foreign terrorist fighter*, *homegrown terrorist fighter*, extrémiste potentiellement violent ou propagandiste de haine. À l'issue de ce délai, soit il est avéré que ces personnes peuvent répondre aux critères de l'article 2, 7°, 8°, 9° ou 11° et elles restent par conséquent enregistrées dans la banque de données commune T.E.R. aussi longtemps que prévu dans l'article 7, § 1, soit cela n'est pas avéré et elles sont supprimées conformément à la procédure visée à l'article 7, § 3. Cette procédure est actuellement prévue à l'article 13 de l'arrêté royal TF et de l'arrêté royal PH.

S'agissant d'une situation transitoire permettant au service de base de rassembler les éléments nécessaires, l'enregistrement de l'entité en pré-enquête n'est possible que pour un délai de maximum 6 mois. Le service de base après au maximum 6 mois doit ou bien avoir reçu les éléments nécessaires à la validation de la situation précise de l'entité en pré-enquête et l'entité en pré-enquête peut être proposée à la validation de l'OCAM, qui valide alors sa situation ou bien il n'y a pas de validation de l'OCAM et le service de base doit conclure qu'il n'y

de dangersevaluatie als bedoeld in artikel 27 ook dat de gegevens worden gecontroleerd.

De mogelijkheid van archivering is aan DRI voorbehouden als technisch beheerder, en aan de operationeel verantwoordelijke. In sommige gevallen gebeurt de archivering automatisch na 30 jaar en valt zij onder de verantwoordelijkheid van DRI. In andere gevallen kan de archivering echter plaatsvinden na een onderzoek van de persoonsgegevens en informatie om na te gaan of deze nog voldoen aan een van de doeleinden waarvoor de gemeenschappelijke gegevensbank is opgezet. In het geval van minderjarigen tussen 12 en 18 jaar die in de gemeenschappelijke gegevens T.E.R. zijn geregistreerd, zal bijzondere aandacht worden besteed aan de koppeling van de registratie van de minderjarige aan de situatie van zijn ouder of daarmee gelijkgestelde persoon. In dit geval zou de archivering vooraf kunnen plaatsvinden. Dit onderzoek en het voorstel tot archivering vallen onder de verantwoordelijkheid van de operationeel verantwoordelijke. In de praktijk worden de entiteiten systematisch in de "lokale taskforce" besproken voordat een besluit tot archivering wordt genomen. Het OCAD bevestigt vervolgens de beslissing aan DRI, met dien verstande dat het OCAD een eindevaluatie moet opstellen die de beslissing bevestigt.

In afwijking van de algemene regel voorzien in artikel 7, § 1, voorziet paragraaf 2 in een verkorting van de maximumtermijn tot 6 maanden voor de gegevens en informatie met betrekking tot een entiteit in "vooronderzoek", d.w.z. die, op het ogenblik van haar registratie in de gegevensbank T.E.R., niet beantwoordt aan de criteria om als een *foreign terrorist fighter*, *homegrown terrorist fighter*, potentieel gewelddadige extremist of haatpropagandist beschouwd te worden. Na afloop van die termijn wordt ofwel aangetoond dat die personen kunnen beantwoorden aan de criteria van artikel 2, 7°, 8°, 9° of 11° en blijven zij bijgevolg in de gemeenschappelijke gegevensbank T.E.R. geregistreerd zo lang als bepaald in artikel 7, § 1, ofwel is dat niet voldoende aangetoond en worden zij uitgewist volgens de procedure voorzien in artikel 7, § 3. Deze procedure is momenteel voorzien in artikel 13 van het koninklijk besluit TF en het koninklijk besluit HP.

Aangezien het om een tijdelijke situatie gaat die de basisdienst toelaat om de nodige elementen te verzamelen, is de registratie van de entiteit in vooronderzoek slechts mogelijk voor een maximumperiode van 6 maanden. De basisdienst moet na maximum 6 maanden ofwel de nodige elementen voor de validatie van de precieze situatie van de entiteit in vooronderzoek hebben ontvangen en de entiteit in vooronderzoek kan ter validatie door OCAD voorgesteld worden die vervolgens haar situatie valideert ofwel is er geen validatie door

a pas d'éléments suffisants pour déterminer plus précisément la situation de l'entité en pré-enquête. Si le délai de 6 mois est écoulé, les données de l'entité en pré-enquête sont supprimées de la banque de données commune T.E.R. Il y a lieu ici de tenir compte des task forces locale (T.F.L.) visées à l'article 31. Ce forum, organisé par arrondissement en associant aussi des magistrats, permet tout particulièrement de discuter des entités se trouvant dans cette situation. L'intérêt d'une banque de données commune est en effet que chaque service apporte les données dont il dispose pour permettre au service de base qui a enregistré l'entité d'assurer sa responsabilité de qualité des données et de ne pas simplement proposer au responsable opérationnel des entités sans suffisamment d'éléments pour une validation fondée de la situation de l'entité concernée.

Dans ce cadre, il faut bien commencer par un enregistrement sans attendre que toutes les données soient disponibles. Bien entendu, cette situation ne peut pas être résiduelle, à défaut d'autre chose. Ce n'est pas l'objectif et c'est pour cela qu'une durée limitée à 6 mois est prévue. Cela n'exonère pas le service de base ayant enregistré l'entité de son obligation de traiter des données adéquates, pertinentes et non excessives.

Le paragraphe 3 concerne le délai d'archivage des données à caractère personnel et informations de 30 ans ainsi que les finalités d'une consultation de ces archives. Par rapport à l'article 44/11/3bis, § 7, de la loi sur la fonction de police, le paragraphe 3 rend obligatoire, et non plus optionnel, l'archivage pour une durée de 30 ans des données à caractère personnel et des informations.

Il faut noter ici qu'il a été tenu compte de l'avis n° 97/2023 de l'Autorité de protection des données du 16 juin 2023 (§ 117) et qu'un effacement anticipé d'une donnée ou information est dès lors possible si cette donnée ou information est fausse ou erronée.

L'accès aux archives se fera sous la forme d'une simple consultation des données à caractère personnel et informations qui y figurent et n'octroie pas un droit de création, un droit de lecture ou d'écriture dans celles-ci. En effet, rien de nouveau n'est créé ou modifié dans les archives.

OCAD en dient de basisdienst te besluiten dat er geen voldoende elementen voorhanden zijn om de situatie van de entiteit in vooronderzoek op een preciezere wijze te bepalen. Wanneer de termijn van 6 maanden verstreken is, worden de gegevens van de entiteit in vooronderzoek bijgevolg uit de gemeenschappelijke gegevensbank T.E.R. gewist. Hierbij dient rekening gehouden te worden met de lokale task forces (L.T.F.) waarnaar in artikel 31 wordt verwezen. Dit forum, dat per arrondissement georganiseerd wordt en dat tevens de magistraten betreft, maakt het meer bepaald mogelijk om over de entiteiten die zich in deze situatie bevinden, te overleggen. Het belang van een gemeenschappelijke gegevensbank bestaat er namelijk in dat elke dienst de gegevens aanbrengt waarover hij beschikt om het aan de basisdienst die de entiteit heeft geregistreerd, mogelijk te maken zijn verantwoordelijkheid op het vlak van de kwaliteit van de gegevens te verzekeren en niet simpelweg een voorstel omtrent de entiteiten te doen aan de operationeel verantwoordelijke zonder dat er voldoende elementen zijn voor een gefundeerde validering van de situatie van de betrokkene entiteit.

In dit kader, moet men wel degelijk registreren zonder te wachten tot op het ogenblik dat alle gegevens beschikbaar zijn. Deze situatie mag welteverstaan geen restcategorie worden, wanneer er voor de rest niks is. Dat is niet de bedoeling en het is daarom dat een beperkte termijn van 6 maanden voorzien werd. Dit ontheft de basisdienst die de entiteit geregistreerd heeft niet van zijn verplichting om toereikende, ter zake dienende en niet overmatige gegevens te verwerken.

Paragraaf 3 heeft betrekking op de termijn van archivering van 30 jaar van de persoonsgegevens en informatie alsmede op de doeleinden van een raadpleging van die archieven. In vergelijking met artikel 44/11/3bis, § 7, van de wet op het politieambt, maakt paragraaf 3 de archivering voor een duur van dertig jaar van de persoonsgegevens en de informatie verplicht en niet langer optioneel.

Hier moet worden opgemerkt dat er rekening werd gehouden met advies nr. 97/2023 van 16 juni 2023 van de Gegevensbeschermingsautoriteit (§ 117) en dat een vroegtijdige verwijdering van een gegeven of van informatie dan ook mogelijk is wanneer dat gegeven of die informatie fout of verkeerd is.

De toegang tot de archieven zal bestaan in een eenvoudige raadpleging van de persoonsgegevens en de informatie die daarin opgenomen zijn en verleent geen creatie-, lees- of schrijfrecht. Er wordt in de archieven immers niets nieuws aangemaakt of niets gewijzigd.

Le traitement des antécédents consiste d'une part à la consultation des archives uniquement dans le cadre des finalités d'enquêtes judiciaires et d'enquêtes de renseignement. Pratiquement, seuls le ministère public, les services de police et les services de renseignement pourront avoir accès aux archives dans le cadre de cette finalité. Pour répondre aux préoccupations de l'Autorité de protection des données (cf. Avis n° 97/2023 du 16 juin 2023, § 116), les finalités de l'utilisation des archives sont clairement définies dans la loi et au vu de ces finalités, comme précisé ci-avant, seuls les services de base ou le ministère public y auront accès.

Ce traitement consiste d'autre part, à la possibilité de transférer les données pertinentes des archives dans l'hypothèse où une personne redevient active. Dans son avis du 13 juillet 2023, le Comité R estime que les modalités de l'archivage et les traitements autorisés sur les données archivées doivent être décrits dans le dispositif (§ 10). À cet égard, il faut préciser que l'article 7, § 3 (ancien § 2), al. 4, détermine déjà les cas dans lesquels la consultation des archives est possible. La consultation est en outre le seul traitement des archives autorisés. Néanmoins, un nouveau paragraphe 4 est inséré et précise dans quel cas, les données archivées pourront de nouveau être visibles dans la banque de données commune.

La procédure de réactivation d'une archive se déroule sous la maîtrise et la responsabilité du responsable opérationnel.

Suite à l'avis du Conseil d'État n° 73.442/2 du 7 juin 2023, l'alinéa précisant que la consultation des archives pour la réalisation de finalités historiques, scientifiques ou statistiques conformément aux dispositions du chapitre X, sous-titre 4, du Titre 3, de la loi relative à la protection des données est supprimé en raison du double emploi de cette disposition avec l'article 4, alinéa 1^{er} du projet.

Suite à l'avis du Conseil d'État n° 73.442/2 du 7 juin 2023 concernant les habilitations au Roi, l'ancien paragraphe qui donnait la possibilité au Roi de déterminer par arrêté royal délibéré en Conseil des ministres, après avis des autorités de contrôle, des règles complémentaires de gestion des données est supprimé. De plus, l'habilitation des règles de gestion des données est aussi prévue à l'article 6.

Pour le reste, il est renvoyé aux travaux parlementaires de la loi du 27 avril 2016 relative à des mesures

De verwerking van de antecedenen bestaat er enerzijds in dat de archieven enkel worden geraadpleegd in het kader van de doeleinden van gerechtelijke onderzoeken en inlichtingenonderzoeken. In de praktijk zullen enkel het openbaar ministerie, de politiediensten en de inlichtingendiensten toegang kunnen hebben tot de archieven in het kader van dat doeleinde. Om te beantwoorden aan de bezorgdheden van de Gegevensbeschermingsautoriteit (cf. Advies nr. 97/2023 van 16 juni 2023, § 116) worden de doeleinden voor het gebruik van de archieven duidelijk gedefinieerd in de wet en, zoals hierboven verduidelijkt en met het oog op die doeleinden, zullen enkel de basisdiensten en het openbaar ministerie ertoe toegang hebben.

Anderzijds behelst die verwerking de mogelijkheid om relevante gegevens van de archieven door te geven ingeval een persoon opnieuw actief wordt. In het advies van 13 juli 2023 is het Comité I van mening dat de archiveringsprocedures en de toegestane verwerkingen van gearcheiverde gegevens in de bepalingen moeten worden beschreven (§ 10). Daartoe moet worden verduidelijkt dat artikel 7, § 3 (voormalig § 2), vierde lid, reeds de gevallen bepaalt waarin de raadpleging van de archieven mogelijk is. De raadpleging is bovendien de enige toegestane verwerking van de archieven. Niettemin wordt een nieuwe paragraaf 4 ingevoegd en wordt er verduidelijkt in welk geval de gearcheiverde gegevens opnieuw zichtbaar kunnen worden in de gemeenschappelijke gegevensbank.

De procedure voor de reactivering van een archief verloopt onder de controle en de verantwoordelijkheid van de operationeel verantwoordelijke.

In navolging van advies nr. 73.442/2 van 7 juni 2023 van de Raad van State wordt het lid ter verduidelijking van de raadpleging van de archieven voor de verwezenlijking van historische, wetenschappelijke of statistische doeleinden overeenkomstig de bepalingen van hoofdstuk X, ondertitel 4 van titel 3, van de wet gegevensbescherming geschrapt wegens het dubbele gebruik van die bepaling met artikel 4, eerste lid, van het ontwerp.

In navolging van advies nr. 73.442/2 van 7 juni 2023 van de Raad van State met betrekking tot de machtigingen van de Koning, wordt de vroegere paragraaf geschrapt die de Koning de mogelijkheid gaf, bij een in Ministerraad overlegd koninklijk besluit en na advies van de toezichthoudende overheden, aanvullende regels inzake het beheer van de gegevens te bepalen. Bovendien wordt in artikel 6 ook in de machtiging van de regels inzake het beheer van de gegevens voorzien.

Voor het overige wordt verwezen naar de parlementaire werkzaamheden van de wet van 27 april 2016 inzake

complémentaires en matière de lutte contre le terrorisme (DOC 54 1727/001, p. 22-23).

Dans son avis n° 97/2023 du 16 juin 2023, l'Autorité de protection des données s'interroge sur le traitement des données archivées (§§ 54 à 57). À ce sujet, il faut rappeler que les archives sont pseudonymisées lorsqu'on se trouve en dehors du cadre des law enforcement car ces derniers ont besoin des informations non pseudonymisées pour l'exercice de leurs missions et des finalités de la banque de données commune en lien avec la lutte contre le terrorisme et l'extrémisme violent (sauf pour les finalités statistiques). Par ailleurs, il n'est pas à exclure qu'une information n'existe plus dans une banque de données d'un service partenaire mais qu'elle soit toujours active dans une autre banque de données. Afin de permettre une saine gestion des données, en évitant que chaque service puisse modifier n'importe quelle donnée enregistrée, dans le cadre de la mise en œuvre de l'habilitation visée à l'article 30, § 4, il sera prévu que seul le service qui a enregistré une donnée peut la modifier, la rectifier et la supprimer. Si un autre service estime qu'une donnée doit être modifiée, rectifiée ou supprimée, il en informe le service qui l'a enregistrée en vue de procéder le cas échéant aux adaptations nécessaires. En cas de différend à ce sujet, le responsable opérationnel en est informé et si le litige subsiste, le responsable opérationnel, après concertation avec les services concernés décide *in fine* en la matière. En outre, par rapport à la remarque formulée au § 58 indiquant que le libellé de la finalité du traitement ultérieur doit également permettre de déterminer la compatibilité de cette finalité avec la finalité pour laquelle les données ont été initialement collectées, il faut rappeler que ce n'est pas parce qu'un service auteur de la donnée l'efface de son système que cette donnée n'est plus utile pour la finalité du service du destinataire (à condition qu'elle soit toujours compatible avec la finalité initiale). Cette compatibilité est examinée au moment de la communication. Par ailleurs, à cet égard, le gouvernement souhaite rappeler qu'un traitement ultérieur pour d'autres finalités (à savoir celles des missions des différents services de base) est permis sur la base de l'article 75, 2°, de la loi cadre en matière de protection des données, qui stipule "les données à caractère personnel (sont) collectées pour des finalités déterminées, explicites et légitimes, et (ne peuvent pas) être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des dispositions légales et réglementaires applicables (...)". Dès lors que le législateur permet le droit de lecture et le droit d'écriture ou l'interrogation directe des services partenaires, il permet que les données de la banque de données commune T.E.R. soient utilisées dans le cadre des finalités propres à chaque service partenaire. C'est d'ailleurs bien dans

aanvullende maatregelen ter bestrijding van terrorisme (DOC 54 1727/001, blz. 22-23).

In advies nr. 97/2023 van 16 juni 2023 heeft de Gegevensbeschermingsautoriteit vragen over de verwerking van de gearchiveerde gegevens (§§ 54 tot 57). Ter zake moet worden herhaald dat de archieven gepseudonimiseerd worden wanneer men zich buiten het kader van law enforcement bevindt. Deze laatste hebben niet-gepseudonimiseerde informatie nodig om hun opdrachten uit te oefenen, alsook de doeleinden van de gemeenschappelijke gegevensbank in verband met de strijd tegen terrorisme en gewelddadig extremisme (behalve statistische doeleinden). Bovendien is het niet uit te sluiten dat informatie niet meer bestaat in een gegevensbank van een partnerdienst, maar nog altijd actief is in een andere gegevensbank. Teneinde een gezond gegevensbeheer mogelijk te maken en te voorkomen dat elke dienst om het even welk geregistreerd gegeven kan wijzigen, wordt in het kader van de tenuitvoerlegging van de machtiging beoogd in artikel 30, § 4, erin voorzien dat enkel de dienst die een gegeven heeft geregistreerd, dat kan wijzigen, verbeteren en verwijderen. Indien een andere dienst van mening is dat een gegeven moet worden gewijzigd, verbeterd of verwijderd, stelt hij de dienst die het heeft geregistreerd daarvan in kennis om in voorkomend geval over te gaan tot de nodige aanpassingen. In geval van geschil ter zake wordt de operationeel verantwoordelijke daarvan op de hoogte gebracht en indien het geschil blijft bestaan, beslist de operationeel verantwoordelijke *in fine* ter zake, na overleg met de betrokken diensten. Met betrekking tot de opmerking in § 58 die vermeldt dat de formulering van het doel van de verdere verwerking het ook mogelijk moet maken de verenigbaarheid met het doel waarvoor de gegevens oorspronkelijk zijn verzameld, vast te stellen, moet er bovendien worden herhaald dat het niet zo is dat een gegeven niet meer nuttig is voor het doeleinde van de dienst van de ontvanger (op voorwaarde dat dit doeleinde steeds verenigbaar is met het oorspronkelijke doeleinde), omdat de dienst die het gegeven oorspronkelijk heeft opgenomen, het verwijdert uit zijn systeem. Die verenigbaarheid wordt onderzocht op het tijdstip van de communicatie. Bovendien, wil de regering ter zake eraan herinneren dat een verdere verwerking voor andere doeleinden (te weten die van de opdrachten van de verschillende basisdiensten) is toegestaan op grond van artikel 75, 2°, van de kaderwet betreffende de bescherming van persoonsgegevens die bepaalt: "persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden [worden] verkregen en niet verder verwerkt op een wijze die, rekening houdend met alle factoren, met name met de toepasselijke en reglementaire bepalingen, onverenigbaar is met die doeleinden.". Daar de wetgever

cette optique que ces services ont reçu la dénomination de “services partenaires”.

Bien entendu, il ne s’agit pas de transformer ces services partenaires en agent de renseignement ou de sécurité qui glaneraient à tout va des données: la loi en projet rappelle en effet que les services partenaires alimentent le cas échéant la banque de données commune T.E.R. qu’avec les données qu’ils traitent dans le cadre de leurs propres missions.

Ensuite, dans son avis du 13 juillet 2023, le comité R juge que la durée maximale de conservation des données au sein de la B.D.C. T.E.R. est trop longue et dépasse dans certains cas la durée de conservation maximale dans les banques de données au sein desquelles les données sont puisées (§ 11). À cet égard, il faut préciser que lors de l’examen de la loi du 27 avril 2016, la Commission de protection de la vie privée a jugé que le délai de 30 ans était acceptable (§§ 61 et 62 de l’avis n° 57/2015 du 16 décembre 2015). En outre, comme l’indiquent les travaux parlementaires de la loi du 27 avril 2016, “(...) Il se peut qu’un service qui est à la base de l’information et qui l’a transmise vers la banque de données commune ait effacé cette donnée à son niveau mais qu’elle soit toujours traitée dans la banque de données commune parce qu’elle présente toujours un intérêt à être partagée dans la banque de données commune dans le cadre des missions visées à l’article 44/2, § 2.

Cette situation résultera de l’existence de finalités différentes entre la banque de données “source” du service à l’origine de l’information et la banque de données commune. Elle peut aussi apparaître en raison de règles de traitement différentes dont par exemple la durée maximale de conservation des données. Ces possibles différences ne doivent pas faire oublier la nécessité de cohérence des données lorsqu’elles portent sur des finalités identiques de traitement. À ce niveau, l’existence de banque de données communes permettra aux services concernés de détecter plus aisément d’éventuelles contradictions dans les données et d’y apporter les solutions nécessaires, ce que ne permet aucunement la situation actuelle avec une séparation totale des données.

de partnerdiensten lees- en schrijfrecht of rechtstreeks vraagrecht toestaat, staat hij toe dat de gegevens van de gemeenschappelijke gegevensbank T.E.R. worden gebruikt in het kader van de doeleinden die eigen zijn aan elke partnerdienst. Het is overigens in die optiek dat die diensten de benaming “partnerdiensten” hebben gekregen.

Natuurlijk is het niet de bedoeling om die partnerdiensten om te vormen tot inlichtingen- of veiligheidsagenten die ongebreideld gegevens zouden sprokkelen: het ontwerp van wet herinnert immers eraan dat de partnerdiensten in voorkomend geval de GGB T.E.R. enkel aanvullen met gegevens die zij verwerken in het kader van hun eigen opdrachten.

Tot slot oordeelt het Comité I in het advies van 13 juli 2023 dat de maximale bewaartermijn voor persoonsgegevens in de gemeenschappelijke gegevensbank T.E.R. bijzonder lang is en in sommige gevallen langer is dan de maximale bewaartermijn in de gegevensbanken waaraan de gegevens worden ontleend (§ 11). In dat verband moet worden verduidelijkt dat tijdens het onderzoek van de wet van 27 april 2016 de Commissie voor de bescherming van de persoonlijke levenssfeer heeft geoordeeld dat de termijn van dertig jaar aanvaardbaar was (§§ 61 en 62 in advies nr. 57/2015 van 16 december 2015). Zoals bovendien te lezen staat in de parlementaire voorbereidingen in het kader van de wet van 27 april 2016: “(...) Het is mogelijk dat een dienst die aan de basis ligt van de informatie en die deze informatie aan de gemeenschappelijke gegevensbank heeft overgemaakt, dit gegeven op zijn niveau heeft uitgewist maar dat dit gegeven nog steeds verwerkt wordt in de gemeenschappelijke gegevensbank omdat het, in het kader van opdrachten bedoeld in artikel 44/2, § 2, nog steeds belangrijk is dit gegeven te delen in de gemeenschappelijke gegevensbank.

Deze situatie zal voortspruiten uit het bestaan van verschillende doeleinden tussen de “bron”-gegevensbank van de dienst die aan de basis van de informatie ligt en de gemeenschappelijke gegevensbank. Zij kan tevens voor komen omwille van verschillende verwerkingsregels waaronder bijvoorbeeld de maximale bewaringstermijn van de gegevens. Deze mogelijke verschillen mogen de noodzaak aan coherentie van de gegevens niet doen vergeten wanneer deze op identieke verwerkingsdoeleinden slaan. Op dit niveau, zal het bestaan van gemeenschappelijke gegevensbanken de verschillende betrokken diensten toelaten om gemakkelijker eventuele tegenstrijdigheden in de gegevens te ontdekken en er de noodzakelijke oplossingen voor aan te brengen, hetgeen de huidige situatie met een totale afscheiding van de gegevens op geen enkele wijze toelaat.

Les phénomènes de terrorisme et d'extrémisme pouvant conduire au terrorisme ne peuvent en effet pas être traités utilement sur des courtes périodes vu que les réponses opérationnelles à apporter sont tributaires d'une compréhension historique, anthropologique et sociétale de ceux-ci.

Il peut en effet s'avérer que des données recueillies prennent plus de sens ou un éclairage différent après de nombreuses années, à la lumière de nouvelles informations ou d'événements nouveaux.

De même, les premières phases d'identification, de recrutement et d'activation de personnes ou de cellules dormantes peuvent être espacées par de nombreuses années. Certaines organisations laissent leurs membres parvenir à des fonctions-clés avant de les solliciter à nouveau.

L'allongement de la durée de vie amène à devoir concevoir l'implication de personnes dans des organisations ou des mouvances qui font l'objet de l'attention légitime des services compétents et dont les données sont traitées dans les banques de données communes sur une durée plus longue correspondant à cette mutation démographique. (...)» (DOC 54 1727/001, pp. 24-25).

Dans son avis du 20 juin 2023, le C.O.C. a également souligné la nécessité d'un suivi strict des délais prévus, et ce par le biais du développement d'un outil ICT, pour que les autorités de contrôle puissent vérifier le bon respect de ces délais. Il recommande ainsi d'inclure dans le projet de loi que le responsable opérationnel reprenne cette évaluation dans le dossier de l'entité concernée, de manière qu'il soit possible pour les autorités de contrôle de vérifier l'évaluation et le délai, et de suivre rigoureusement ces délais dans une application informatique.

Dans son avis précité, l'Autorité de protection des données estime quant à lui que la vérification des conditions de conservation dans la BDC ou dans les archives de la BDC doit intervenir à intervalle plus régulier et recommande une vérification annuelle et un archivage après 5 ans de vérifications infructueuses (§ 118). Toutefois, le projet prévoit déjà un examen sur une base régulière sur base de critères qui sont plus rigoureux que ceux suggérés par l'Autorité.

À cet égard, il faut rappeler qu'il existe plusieurs mécanismes permettant de contrôler le respect des délais comme le processus de validation récurrent des entités par l'OCAM, le système de ventilation, l'actualisation de

Fenomenen van terrorisme en van extremisme dat kan leiden tot terrorisme kunnen namelijk niet op een nuttige wijze verwerkt worden over korte periodes omdat de er aan te geven operationele antwoorden afhankelijk zijn van een historisch, antropologisch en maatschappelijk begrip ervan.

Het kan met name blijken dat de ingewonnen gegevens na talrijke jaren een grotere betekenis of een verschillende duiding krijgen in het licht van nieuwe informatie of nieuwe gebeurtenissen.

Op dezelfde wijze kan er een groot tijdsverschil van verschillende jaren bestaan tussen de eerste fasen van identificatie, rekrutering en activering van personen of slapende cellen. Sommige organisaties laten hun leden sleutelfuncties bereiken alvorens hen opnieuw in te schakelen.

De verlenging van de levensduur draagt bij tot de verplichting om de betrokkenheid te begrijpen van de personen bij de organisatie of bij de bewegingen, die het voorwerp uitmaken van een gerechtvaardigde aandacht van de bevoegde diensten en van wie de gegevens verwerkt worden in de gemeenschappelijke gegevensbanken over een langere duur die overeenstemt met deze demografische wijziging. (...)» (DOC 54 1727/001, pp. 24-25).

Het COC heeft in het advies van 20 juni 2023 eveneens de benadrukt dat een strikte opvolging van de voorziene termijnen nodig is door middel van de ontwikkeling een ICT-applicatie, zodat de toezichthoudende overheden de goede naleving van die termijnen kunnen controleren. Het beveelt dan ook aan om in het wetsontwerp op te nemen dat de operationeel verantwoordelijke deze evaluatie opneemt in het dossier van de betreffende entiteit, opdat een verificatie van de evaluatie en de termijn door de toezichthoudende overheden mogelijk is, evenals een strikte opvolging van deze termijnen aan de hand van een ICT applicatie.

In het voormeld advies is de Gegevensbeschermingsautoriteit dan weer van mening dat de omstandigheden van de opslag in de GGB of in de archieven van de GGB regelmatig moeten worden gecontroleerd en beveelt een jaarlijkse audit en archivering aan na 5 jaar van onsuccesvolle verificaties (§ 118). Het ontwerp voorziet evenwel eens in regelmatig onderzoek op grond van criteria die nauwgezetter is dan degene die de autoriteit voorstelt.

In dat verband moet worden herhaald dat er verschillende mechanismen bestaan om de naleving van de termijnen te controleren, zoals het herhaalde valderingsproces van de entiteiten door het OCAD, het

l'évaluation de la menace par l'OCAM deux fois par an ou encore les discussions d'une entité en TFL. Toutes ces procédures sont assorties de dates qui sont accessibles aux autorités de contrôle et qui leur permettent donc d'exercer leur mission.

Art. 8

L'article 8 concerne les fichiers de journalisation des traitements effectués dans la banque de données commune. Il reprend l'article 44/4, § 2, de la loi sur la fonction de police.

Toutefois, n'est pas repris ici, le § 2, alinéa 1^{er}, de l'article 44/4 de la loi sur la fonction de police. En effet, cet alinéa donne compétence aux ministres de l'Intérieur et de la Justice pour déterminer par directives contraignantes les mesures nécessaires en vue d'assurer la gestion et la sécurité des données à caractère personnel et des informations traitées dans la banque de données commune. Or, cette compétence est déjà accordée au Roi par l'article 6, § 2, alinéa 4. Il n'y a dès lors plus lieu de le reprendre ici.

L'énumération des traitements qui doivent faire l'objet d'une journalisation est exhaustive. Suite à l'avis n° 97/2023 du 16 juin 2023 de l'Autorité de protection des données, notamment en ce qui concerne l'extraction (§§ 22-23) et afin d'éviter tout doute, la liste des traitements pour lesquelles des fichiers de journalisation doivent être établis est celle de l'article 4, 2), du règlement général sur la protection des données.

L'actuel article 44/4, § 2, alinéa 3, 1° à 4°, de la loi sur la fonction de police est repris à l'article 8, § 1^{er}, alinéa 2, 1° à 4°. La seule modification apportée à ce texte concerne le 2°. En effet, actuellement, les fichiers de journalisation de consultation et de communication permettent d'établir les catégories de personnes qui ont consulté les données à caractère personnel, ainsi que l'identification de la personne qui a consulté ces données. Or, il existe des services opérationnels, à savoir les services de renseignements, qui, dans le but de protéger leurs sources et les membres de leur personnel, disposent d'un code d'identification unique pour l'ensemble des services dans les banques de données externes à leurs services. Les fichiers de journalisation de la banque de données commune T.E.R. permettent donc uniquement pour ces services d'identifier quel service (renseignement civil ou militaire) a fait quoi à quel moment et pourquoi. La journalisation des accès individuels se fait dès lors en interne au niveau de chaque service de renseignements. Pour couvrir tous les cas de figure, la nouvelle formulation prévoit que

verdelingssysteem, de update van de dreigingsevaluatie door het OCAD tweemaal per jaar of de besprekingen van een entiteit in de LTF. Al die procedures zijn gekoppeld aan data die toegankelijk zijn voor de toezichthoudende overheden waardoor ze hun opdracht kunnen uitoefenen.

Art. 8

Artikel 8 heeft betrekking op de logbestanden van de verwerkingen uitgevoerd in de gemeenschappelijke gegevensbank. Het herneemt artikel 44/4, § 2, van de wet op het politieambt.

Artikel 44/4, § 2, eerste lid, van de wet op het politieambt is hier evenwel niet hernomen. Dat lid geeft de ministers van Binnenlandse Zaken en van Justitie immers de bevoegdheid om bij dwingende richtlijn de maatregelen te bepalen die nodig zijn om het beheer en de veiligheid van de persoonsgegevens en de informatie die worden verwerkt in de gemeenschappelijke gegevensbank, te verzekeren. Die bevoegdheid is evenwel reeds toegekend aan de Koning bij artikel 6, § 2, vierde lid. Het moet hier dan ook niet worden hernomen.

De opsomming van de verwerkingen die het voorwerp moeten zijn van een logging is exhaustief. In navolging van advies nr. 97/2023 van 16 juni 2023 van de Gegevensbeschermingsautoriteit, inzonderheid wat de extractie betreft (§§ 22-23) en om enige twijfel te voorkomen, is de lijst van verwerkingen waarvoor de loggingbestanden moeten worden aangemaakt, degene van artikel 4, 2), van de algemene verordening gegevensbescherming.

Het huidige artikel 44/4, § 2, derde lid, 1° tot en met 4°, van de wet op het politieambt wordt overgenomen in artikel 8, § 1, tweede lid, 1° tot en met 4°. De enige wijziging die aan die tekst werd aangebracht, betreft 2°. De logbestanden van de raadpleging en de mededeling maken het thans immers mogelijk om vast te stellen welke categorieën van personen de persoonsgegevens hebben geraadpleegd, alsook de identificatie vast te stellen van de persoon die die gegevens heeft geraadpleegd. Er zijn dus operationele diensten, met name de inlichtingendiensten, die, om hun bronnen en personeelsleden te beschermen, beschikken over een unieke identificatiecode voor alle diensten in de gegevensbanken buiten hun diensten. De logbestanden van de gemeenschappelijke gegevensbank T.E.R. bieden dus enkel voor die diensten de mogelijkheid om te identificeren welke dienst (burgerlijke of militaire inlichtingen) wat wanneer en waarom heeft gedaan. Het loggen van de individuele toegang gebeurt dus intern bij elke inlichtingendienst. Om alle gevallen te dekken voorziet de nieuwe formulering erin dat de gegevens of

les données ou codes d'identification des personnes ou des services ayant accès à la banque de données commune font l'objet de la journalisation.

L'article 8, § 1, alinéa 3, vise la conservation de la journalisation des traitements réalisés dans la banque de données commune durant 30 ans, à partir de la réalisation du traitement effectué. Cette disposition simplifie, au niveau de son libellé, l'actuel article 44/11/3b/s, § 6, de la loi sur la fonction de police. Le libellé a également été adapté suite à l'avis de l'Autorité de protection des données n° 97/2023 du 20 juin 2023 (§ 22). Cette modification permet également de répondre à la préoccupation du Comité R (§ 12 de l'avis du 13 juillet 2023).

Dans son avis du 13 juillet 2023, le Comité R recommande également que la durée de conservation des données de journalisation soit nécessairement calquée sur celle des données concernées par les traitements (§ 13). Sur ce point, il faut rappeler que le délai de conservation des données de journalisation retenu coïncide avec la durée retenue de conservation des données au sein de la banque de données commune (cf. avis n° 57/2015 du 16 décembre 2015 de la Commission de la protection de la vie privée, § 67 et DOC 54 1727/001, p. 23).

Conformément à l'avis du Conseil d'État 73.442/2 du 7 juin 2023 et à l'avis de l'Autorité de protection des données n° 97/2023 du 20 juin 2023 (§ 22), dans la mesure où l'énumération des traitements qui doivent faire l'objet d'une journalisation est exhaustive, il convient d'omettre l'habilitation du Roi à déterminer d'autres types de traitements pour lesquels les fichiers de journalisation sont établis.

Les paragraphes 2 à 3, de l'article 8 reprennent l'article 44/4, § 2, alinéas 5, 6, 7 et 9, de la loi sur la fonction de police. Toutefois, il n'est plus prévu que les procédures soient soumises à l'avis des autorités de contrôle car cela n'est pas nécessaire dans le cadre de procédures internes d'accès et cela les simplifie. Désormais, il est aussi précisé que le responsable opérationnel, en concertation avec le gestionnaire, d'une part, adopte les mesures appropriées pour assurer la sécurité des fichiers de journalisation (§ 2) et d'autre part, adopte des procédures d'accès aux fichiers de journalisation, qui garantissent la nécessité et la proportionnalité de l'accès aux données de journalisation (§ 3). En ce qui concerne la concertation entre le gestionnaire et le responsable opérationnel visé dans ces deux paragraphes, le Comité R propose de remplacer cette formulation par l'exigence d'obtenir un avis, éventuellement conforme, du responsable opérationnel avant la décision du gestionnaire (§ 17). Cependant, il n'est pas question ici d'une

identificatiecodes van de personen of de diensten die toegang hebben tot de gemeenschappelijke gegevensbank, het voorwerp uitmaken van logbestanden.

Artikel 8, § 1, derde lid, beoogt de bewaring van de logbestanden van de verwerkingen uitgevoerd in de gemeenschappelijke gegevensbank gedurende dertig jaar, vanaf de realisatie van de uitgevoerde verwerking. Deze bepaling vereenvoudigt, op het gebied van de formulering ervan, het huidige artikel 44/11/3b/s, § 6, van de wet op het politieambt. Het opschrift werd eveneens aangepast naar aanleiding van advies nr. 97/2023 van 20 juni 2023 van de Gegevensbeschermingsautoriteit (§ 22). Die wijziging kan eveneens een antwoord zijn op de bezorgdheid van het Comité I (§ 12 van het advies van 13 juli 2023).

In het advies van 13 juli 2023 beveelt het Comité I eveneens aan dat de bewaartermijn voor logginggegevens noodzakelijkerwijs dezelfde moet zijn als voor de gegevens waarop de verwerkingen betrekking hebben (§ 13). Op dat punt moet worden herhaald dat de bewaartermijn van de bijgehouden logginggegevens samenvalt met de weerhouden duur van de bewaring van de gegevens in de gemeenschappelijke gegevensbank (cf. advies nr. 57/2015 van 16 december 2015 van de Commissie voor de bescherming van de persoonlijke levenssfeer, § 67, en DOC 54 1727/001, blz. 23).

Overeenkomstig advies nr. 73.442/2 van 7 juni 2023 van de Raad van State en advies nr. 97/2023 van 20 juni 2023 van de Gegevensbeschermingsautoriteit (§ 22) moet de machtiging van de Koning om andere soorten verwerking te bepalen waarvoor loggingbestanden worden aangemaakt, worden weggelaten, aangezien de opsomming van de verwerkingen die moeten worden gelogd exhaustief is.

Paragrafen 2 tot en met 3, van artikel 8 hebben artikel 44/4, § 2, vijfde, zesde, zevende en negende lid, van de wet op het politieambt overgenomen. Niettemin wordt er niet langer in voorzien dat de procedures onderworpen zijn aan het advies van de toezichthoudende overheden aangezien dit niet nodig is in het kader van de interne toegangsprocedures en het deze procedures vereenvoudigt. Voortaan wordt ook gepreciseerd dat de operationeel verantwoordelijke, in overleg met de beheerder, de gepaste maatregelen neemt om de veiligheid van de logbestanden te verzekeren (§ 2) en hij tevens procedures voor de toegang tot de logbestanden instelt, die de noodzaak en de proportionaliteit van de toegang tot de logginggegevens waarborgen (§ 3). Voor het overleg tussen de beheerder en de operationeel verantwoordelijk beoogd in die twee paragrafen stelt Comité I voor om deze formulering te vervangen door de vereiste om advies in te winnen, eventueel met instemming van de operationele verantwoordelijke, voorafgaand

quelconque influence du responsable opérationnel sur la décision du gestionnaire ou inversement. En effet, ces deux acteurs se consultent nécessairement pour l'adoption des règles. Il s'agit d'un travail collaboratif qui existe actuellement et fonctionne de manière correcte.

Le paragraphe 4, a quant à lui été adapté pour renvoyer aux articles qui traitent de la journalisation. En effet, actuellement, l'article 44/4, § 4, prévoit que les ministres de l'Intérieur et de la Justice, déterminent par directives contraignantes les mesures nécessaires en vue d'assurer la gestion et la sécurité dont notamment les aspects relatifs à la fiabilité, la confidentialité, la disponibilité, la traçabilité et l'intégrité des données à caractère personnel et des informations traitées dans la banque de données commune. Tous ces aspects sont maintenant réglés en partie par la loi, il est donc renvoyé aux paragraphes y relatifs. De même, les mots "désignés en droit et en faits" sont supprimés car c'est le Roi qui désigne le gestionnaire. En outre, ces termes ne se justifient pas en dehors de la loi sur la fonction de police dont les deux derniers alinéas de l'article 44/4, § 2, distinguent les autres bases de données de la police de la banque de données commune.

Dans son avis précité, l'Autorité de protection des données estime "qu'il y a lieu de prévoir que la collecte des données susceptibles d'être enregistrées dans la BDC doit avoir été journalisée. Les normes organiques des services disposant d'un droit d'écriture devront donc être modifiées en ce sens" (§ 24). Ce commentaire de l'APD nous offre l'opportunité de préciser que l'identification des responsables du traitement de la banque de données commune T.E.R. est prévue à l'article 30. Les responsables du traitement doivent logiquement se conformer au RGPD et à la loi sur la protection des données, l'avant-projet de loi n'entendant pas exonérer les responsables du traitement de leurs responsabilités, sous réserve des règles particulières spécifiées dans l'avant-projet. Dès lors, le responsable du traitement reste soumis au principe de "responsabilité" et doit être en mesure de démontrer son respect des principes relatifs au traitement des données à caractère personnel (art. 5.2 du RGPD).

De même, l'Autorité de protection des données estime que le projet de loi et les normes organiques des services partenaires doivent prévoir les modalités du contrôle des fichiers de journalisation pour les traitements "locaux" (§§ 25-26). Or, ces modalités ne découlent pas du RGPD. Chaque service partenaire est tenu de

aan de beslissing van de beheerder. (§ 17). Het is hier echter niet de kwestie van eender welke invloed van de operationeel verantwoordelijke op de beslissing van de beheerder of omgekeerd. Die twee actoren overleggen immers noodzakelijkerwijs over de regels die worden goedgekeurd. Het gaat om een samenwerking die reeds bestaat en op correcte wijze functioneert.

Paragraaf 4 werd dan weer aangepast om te verwijzen naar de artikelen over de logging. Artikel 44/4, § 4, bepaalt nu immers dat de minister van Binnenlandse Zaken en de minister van Justitie bij bindende richtlijnen de vereiste maatregelen kunnen bepalen met het oog op het beheer en de beveiliging, waaronder inzonderheid de aspecten in verband met de betrouwbaarheid, de vertrouwelijkheid, de beschikbaarheid, de traceerbaarheid, en de integriteit van de persoonsgegevens en de informatie verwerkt in de gemeenschappelijke gegevensbank. Al die aspecten worden nu deels bij wet geregeld, dus wordt er verwezen naar de desbetreffende paragrafen. Ook de woorden "aangewezen in rechte of in feite" worden geschrapt, aangezien het de Koning is die de beheerder aanwijst. Die woorden zijn bovendien zinloos buiten de wet op het politieambt, waarvan de laatste twee leden van artikel 44/4, § 2, het onderscheid maken tussen de gemeenschappelijke gegevensbank en de andere gegevensbanken van de politie.

In het voormeld advies is de Gegevensbeschermingsautoriteit daarom van mening "dat moet worden bepaald dat het verzamelen van gegevens die [...] in de GGB zullen worden geregistreerd, in een logbestand zijn opgenomen. De organieke normen van de diensten met schrijfrechten zullen daarom dienovereenkomstig moeten worden aangepast." (§ 24). Die opmerking van de GBA biedt ons de mogelijkheid om te verduidelijken dat de identificatie van de verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank T.E.R. wordt bepaald in artikel 30. De verwerkingsverantwoordelijken moeten zich logischerwijze houden aan de AVG en de wet gegevensbescherming, aangezien het voorontwerp niet de bedoeling heeft de verwerkingsverantwoordelijken te ontheffen van hun verantwoordelijkheden, onder voorbehoud van de in het voorontwerp bepaalde bijzondere regels. De verwerkingsverantwoordelijke blijft dan ook onderworpen aan het beginsel van "verantwoordelijkheid" en moeten in staat zijn om zijn naleving van de beginselen met betrekking tot de verwerking van de persoonsgegevens aan te tonen (art. 5.2 van de AVG).

De Gegevensbeschermingsautoriteit is ook van mening dat het ontwerp en de organieke normen van de partnerdiensten voor de "lokale" verwerking de procedures voor het controleren van de logbestanden moeten omvatten (§§ 25-26). Die nadere regels vloeien echter niet voort uit de AVG. Elke partnerdienst moet in die

prévoir ces modalités de contrôle selon la politique qui lui est propre et doit en répondre devant son autorité de contrôle. Ainsi, ce contrôle s'organise spécifiquement par chaque autorité compétente.

Art. 9

La possibilité d'établir une interconnexion entre différentes banques de données, telle que prévue à l'article 44/4, § 4, de la loi sur la fonction de police est prévue dans le cadre de la banque de données commune T.E.R. L'interconnexion constitue un traitement de données qui n'existe pas à l'heure actuelle pour la banque de données commune T.E.R. mais qui pourrait être utile à l'avenir pour se connecter à d'autres banques de données existantes gérées par les services de base ou les services partenaires dans le cadre de leurs missions légales (cf. paragraphe 1^{er}) ou les sources authentiques de données visées au paragraphe 2.

L'objectif d'une telle possibilité d'interconnexion est, notamment d'enrichir la banque de données commune T.E.R. avec les données d'autres bases de données existantes sans devoir réintroduire manuellement ces données dans la banque de données commune T.E.R. Cela permettrait une simplification, une mise à jour plus rapide des données, ainsi qu'un allègement de la charge de travail des services concernés et d'éviter les erreurs résultant d'une introduction manuelle des données. Par ailleurs, une interconnexion offrirait l'avantage d'avoir un accès à des données provenant directement du service à la source de celles-ci. Ce qui garantit de disposer des données les plus actuelles et plus fiables possibles. Il faut rappeler que les données enregistrées doivent être adéquates, pertinentes et non excessives au regard des finalités définies dans la loi en ce qui concerne la banque de données commune.

L'intégrité des données et des réseaux doit cependant bien entendu être respectée, notamment en ce qui concerne les banques de données qui contiennent des données classifiées au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. En effet, ces banques de données font l'objet d'homologations par des autorités compétentes en matière de sécurité et doivent satisfaire à des règles de sécurité renforcées notamment sur le plan de leurs connexions. Ces homologations sont absolument nécessaires pour permettre les échanges sur le plan international. Ainsi, il est entendu que les données classifiées ne pourront pas faire l'objet d'une telle interconnexion. *A contrario*, les données non

nadere controleregels voorzien al naargelang van zijn eigen beleid en moet daarover verantwoording afleggen aan zijn toezichhoudende overheid. Die controle wordt dus specifiek per bevoegde autoriteit georganiseerd.

Art. 9

In het kader van de gemeenschappelijke gegevensbank T.E.R. wordt voorzien in de mogelijkheid tot het maken van een koppeling tussen verschillende gegevensbanken, zoals bepaald in artikel 44/4, § 4, van de wet op het politieambt. De koppeling is een vorm van gegevensverwerking die thans niet bestaat voor de gemeenschappelijke gegevensbank T.E.R., maar die in de toekomst nuttig zou kunnen zijn om verbinding te maken met andere, bestaande gegevensbanken die door de basisdiensten of partnerdiensten worden beheerd in het kader van hun wettelijke opdrachten (cf. paragraaf 1) of authentieke gegevensbronnen als bedoeld in paragraaf 2.

De doelstelling van een dergelijke mogelijkheid tot koppeling is inzonderheid de gemeenschappelijke gegevensbank T.E.R. te verrijken met de gegevens van andere bestaande gegevensbanken zonder die gegevens opnieuw manueel in de gemeenschappelijk gegevensbank T.E.R. te moeten invoeren. Dit zou een vereenvoudiging, een snellere bijwerking van de gegevens en een verlichting van de werklast van de betrokken diensten mogelijk maken en het mogelijk maken om fouten ten gevolge van het handmatig invoeren van gegevens voorkomen. Een koppeling zou overigens het voordeel bieden van toegang te hebben tot gegevens die rechtstreeks afkomstig zijn van de dienst aan de bron van de gegevens, waardoor men kan beschikken over de meest recente en betrouwbare gegevens mogelijk. Ter herinnering: de geregistreerde gegevens moeten toereikend, ter zake dienend en niet overmatig zijn in verhouding tot de in de wet bepaalde doelmatigheden met betrekking tot de gemeenschappelijke gegevensbank.

De integriteit van de gegevens en van de netwerken moet uiteraard in acht worden genomen, met name wat betreft de gegevensbanken die geclassificeerde gegevens bevatten in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen. Die gegevensbanken zijn immers onderworpen aan homologaties van bevoegde beveiligingsinstanties en moeten voldoen aan doorgedreven beveiligingsregels, met name wat de koppelingen ervan betreft. Die homologaties zijn absoluut noodzakelijk om de uitwisselingen op internationaal vlak mogelijk te maken. Het spreekt aldus voor zich dat de geclassificeerde gegevens niet in aanmerking kunnen komen voor een dergelijke koppeling.

classifiées traitées par les services de renseignements et de sécurité peuvent être interconnectées avec la banque de données commune T.E.R., toujours dans le respect de l'intégrité des données et des réseaux. A ce sujet, le Comité R a fait part de ses préoccupations dans son avis du 13 juillet 2023 (§ 15). Il convient de préciser que le but de l'interconnexion n'est pas de modifier la législation relative aux services de renseignement et de sécurité ou la loi sur la fonction de police. Il va sans dire qu'un arrêté d'exécution relatif aux services de renseignements tiendra compte de la loi cadre en la matière et que donc l'interconnexion se fera dans le respect de cette loi.

À noter que pour ce qui concerne les données qui relèvent de la sécurité nationale, un protocole technique sera en outre conclu avec les services de renseignement et de sécurité.

Il faut préciser que l'interconnexion entre la banque de données commune T.E.R. et d'autres banques de données gérées par les services de base ou les services partenaires dans le cadre de leurs missions légales, peut être bidirectionnelle. Ainsi, cette interconnexion peut permettre d'enrichir/ de consulter la banque de données commune T.E.R. avec les données d'autres bases de données existantes et inversement.

Une interconnexion entre la banque de données commune T.E.R. et tout autre banque de données se ferait au cas par cas et bien entendu, après avis des responsables du traitement des banques de données concernés par cette interconnexion. En outre, elle doit être faisable sur le plan technique et la transmissions des données doit se faire de manière structurée.

Le paragraphe 2 de cet article vise spécifiquement l'interconnexion entre la banque de données commune T.E.R. et quatre bases de sources authentiques de données: le Registre national des personnes physiques, la Banque carrefour des entreprises, le répertoire-matricule des véhicules et le Casier judiciaire central. L'objectif est d'éviter que chaque service qui a un droit de lecture et d'écriture ne doive individuellement s'adresser au gestionnaire de ces bases de données pour obtenir l'accès aux données pertinentes de ces sources authentiques.

À noter que l'interconnexion ne se fera dans cette hypothèse que dans un seul sens, à savoir que les données pertinentes de ces sources authentiques seront consultées et utilisées dans la banque de données commune T.E.R. et pas l'inverse, bien évidemment.

Cette disposition s'inscrit dans la lignée des recommandations de la "Commission d'enquête parlementaire

A contrario kunnen de niet-geclassificeerde gegevens die verwerkt worden door de inlichtingen- en veiligheidsdiensten gekoppeld worden met de gemeenschappelijke gegevensbank T.E.R., steeds met inachtneming van de integriteit van de gegevens en de netwerken. Het Comité I heeft daaromtrent zijn bezorgdheid geuit in het advies van 13 juli 2023 (§ 15). Er moet worden verduidelijkt dat het niet de bedoeling van de koppeling is om de wetgeving inzake de inlichtingen- en veiligheidsdiensten of de wet op het politieambt te wijzigen. Uiteraard zal een uitvoeringsbesluit inzake de inlichtingendiensten rekening houden met de kaderwet ter zake en moet de koppeling gebeuren met inachtneming van die wet.

Er zij op gewezen dat wat de gegevens inzake de nationale veiligheid betreft, ook een technisch protocol zal worden gesloten met de inlichtingen- en veiligheidsdiensten.

Er moet worden verduidelijkt dat, de koppeling tussen de gemeenschappelijke gegevensbank T.E.R. en andere gegevensbanken die worden beheerd door de basisdiensten of door de partnerdiensten in het kader van hun wettelijke opdrachten, in de twee richtingen kan gaan. Aldus kan die koppeling ervoor zorgen dat de gemeenschappelijke gegevensbank T.E.R. verrijkt// geraadpleegd wordt met de gegevens van andere bestaande gegevensbanken, en omgekeerd.

Een koppeling tussen de gemeenschappelijke gegevensbank T.E.R. en elke andere gegevensbank zou geval per geval worden beslist, uiteraard na advies van de verwerkingsverantwoordelijken van de bij deze koppeling betrokken gegevensbanken. Bovendien moet het technisch haalbaar zijn en moeten de gegevens op een gestructureerde manier worden doorgegeven.

Paragraaf 2 van dit artikel verwijst specifiek naar de koppeling tussen de gemeenschappelijke gegevensbank T.E.R. en vier authentieke gegevensbronnen: het Rijksregister van natuurlijke personen, de Kruispuntbank van Ondernemingen, het kentekenplaatregister van de voertuigen en het Centraal Strafregister. Het doel is te voorkomen dat elke dienst met een leesrecht en een schrijfrecht zich individueel tot de beheerder van deze databanken moet wenden om toegang te krijgen tot de relevante gegevens uit deze authentieke bronnen.

Er zij op gewezen dat de koppeling in dat geval slechts eenrichtingsverkeer zal zijn, d.w.z. de relevante gegevens uit deze authentieke bronnen zullen worden geraadpleegd en gebruikt in de gemeenschappelijke gegevensbank T.E.R. en uiteraard niet omgekeerd.

Deze bepaling ligt in de lijn van de aanbevelingen van de "parlementaire onderzoekscommissie belast met het

chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles". La Commission parlementaire a ainsi mis en évidence le besoin d'un échange optimal des données collectées entre les services de sécurité et une gestion intégrée de l'information.

L'alinéa 2 du paragraphe 1^{er} habilite le Roi à déterminer après avis des responsables du traitement des banques de données visées et des autorités de contrôle, les modalités d'interconnexion. La recommandation du C.O.C. du 20 juin 2023 a été suivie concernant la demande d'avis des autorités de contrôle lorsque le Roi mettre en œuvre son habilitation. Par ailleurs, dans son avis n° 97/2023 du 16 juin 2023, l'Autorité de protection de données estime que les finalités de l'interconnexion et les catégories de données à caractère personnel interconnectées doivent figurer dans la loi et non pas dans un arrêté royal (§§ 20-21 et 40). Le Comité R a fait la même remarque dans son avis du 13 juillet 2023 (§ 14). Ce point a été suivi. Les finalités de l'interconnexion ainsi que les catégories de données à caractère personnel interconnectées sont celles de la banque de données commune T.E.R. Il est donc renvoyé à ces finalités dans l'article 9, § 1^{er}. En ce qui concerne les catégories de données interconnectées, il est toutefois nécessaire qu'un arrêté royal détermine quelles seront les données précises qui seront interconnectées entre les deux banques de données concernées. Par ailleurs, cet arrêté royal sera soumis à l'Autorité de protection des données.

En outre, en ce qui concerne les banques de données gérées par le ministère public, l'accord du Collège du ministère public sera nécessaire avant que le Roi ne prenne un arrêté concernant l'interconnexion des systèmes de traitement du Ministère public avec la banque de données commune T.E.R. et de la banque de données commune T.E.R. avec les systèmes de traitement du Ministère public. Cela se justifie par la position particulière et l'indépendance du ministère public telles que prévues à l'article 151 de la Constitution, ainsi que nécessité de pouvoir sauvegarder à tout moment le secret de l'information tel que prévu à l'articles 28quinquies du Code d'instruction criminelle.

Art. 10

L'article 44/11/3bis, § 8, de la loi sur la fonction de police est transféré à l'article 10. Il permet au Roi de

onderzoek naar de omstandigheden die hebben geleid tot de terroristische aanslagen van 22 maart 2016 in de luchthaven Brussel-Nationaal en in het metrostation Maalbeek te Brussel". De parlementaire commissie heeft aldus onderstreept dat een optimale uitwisseling van de verzamelde gegevens tussen de veiligheidsdiensten en een geïntegreerd beheer van de informatie noodzakelijk zijn.

Paragraaf 1, tweede lid, machtigt de Koning om na advies van de verwerkingsverantwoordelijken van de betrokken gegevensbanken en de toezichthoudende overheden de nadere regels van de koppeling te bepalen. De aanbeveling van het COC van 20 juni 2023 werd gevolgd met betrekking tot het verzoek om advies van de toezichthoudende overheden wanneer de Koning zijn bevoegdheid ten uitvoer legt. In het advies nr. 97/2023 van 16 juni 2023 is de Gegevensbeschermingsautoriteit van mening dat de doeleinden van onderlinge koppeling en de categorieën van persoonsgegevens die onderling worden gekoppeld, moeten worden opgenomen in de wet en niet in een koninklijk besluit (§§ 20-21 en 40). Het Comité I heeft dezelfde opmerking geformuleerd in het advies van 13 juli 2023 (§ 15). Dat punt werd gevolgd. De doeleinden van de onderlinge koppeling alsook de categorieën van persoonsgegevens die onderling worden gekoppeld, zijn die van de gemeenschappelijke gegevensbank T.E.R. Er wordt dan ook verwezen naar die doeleinden in artikel 9, § 1. Wat de categorieën van persoonsgegevens die worden gekoppeld betreft, is het evenwel noodzakelijk dat een koninklijk besluit bepaalt welke de precieze gegevens zijn die worden gekoppeld tussen de twee betrokken gegevensbanken. Bovendien zal dat koninklijk besluit worden voorgelegd aan de Gegevensbeschermingsautoriteit.

Voorts is, voor wat de door het openbaar ministerie beheerde gegevensbanken betreft, het akkoord van het College van het openbaar ministerie noodzakelijk alvorens de Koning een besluit neemt betreffende de koppeling van de verwerkingssystemen van het openbaar ministerie met de gemeenschappelijke gegevensbank T.E.R. en van de gemeenschappelijke gegevensbank T.E.R. met de verwerkingssystemen van het openbaar ministerie. De verantwoording daarvoor is de bijzondere positie en de onafhankelijkheid van het openbaar ministerie zoals bepaald in artikel 151 van de Grondwet en de noodzaak om te allen tijde het geheim van het opsporingsonderzoek zoals bedoeld in de artikelen 28quinquies van het Wetboek van Strafvordering te vrijwaren.

Art. 10

Artikel 44/11/3bis, § 8, van de wet op het politieambt wordt omgezet naar artikel 10. Hierdoor kan de Koning

fixer d'autres modalités de gestion de la banque de données commune. Il s'agit d'un maintien du dispositif existant dont le libellé a été simplifié par l'utilisation de la voie active plutôt que la voie passive.

Contrairement à ce que suggère le Conseil d'État dans son avis 73.442/2 du 7 juin 2023, cette habilitation au Roi est maintenue. En effet, comme déjà précisé dans le cadre des travaux parlementaires de la loi du 27 avril 2016 "relative à des mesures complémentaires en matière de lutte contre le terrorisme", il est nécessaire de conserver une certaine souplesse pour pouvoir réagir à une jurisprudence d'autorités nationales ou internationales de contrôle (DOC 54 1727/001, p. 25-26). Par ailleurs, cette disposition donne la flexibilité nécessaire pour une adaptation des modalités complémentaires de gestion de la banque de données commune en raison des évolutions technologiques qui ne peuvent pas être anticipées à ce stade.

Section 4

Gestionnaire et responsable opérationnel

Comme c'est le cas actuellement, deux autres fonctions clefs propres à la banque de données commune T.E.R. sont créées: le gestionnaire et le responsable opérationnel.

Il est apparu important pour une banque de données alimentée et consultée par de multiples partenaires de prévoir des fonctions clefs ayant des missions précises pour assurer le bon fonctionnement quotidien de la banque de données.

À noter que suite à l'avis 73.442/2 du Conseil d'État du 7 juin 2023 en ce qui concerne les habilitations au Roi, l'article qui habilitait le Roi à déterminer des missions spécifiques du gestionnaire et du responsable opérationnel a été supprimé.

Art. 11

L'article 11 concerne le gestionnaire de la banque de données commune ainsi que ses missions. Dans un souci de rassembler l'ensemble des missions du gestionnaire dans un seul texte légal, cet article reprend non seulement le contenu de l'article 44/11/3bis, § 9, de la loi sur la fonction de police mais également celui de l'article 3 de l'arrêté royal "TF" et de l'arrêté royal "PH" en ce qui concerne ses missions. L'ordre des missions a également été revu dans un souci de cohérence. Le

andere nadere beheersregels van de gemeenschappelijke gegevensbank bepalen. De bestaande bepaling wordt behouden, maar de formulering is verduidelijkt door in plaats van de passieve vorm de actieve vorm te gebruiken.

In tegenstelling tot wat de Raad van State suggereert in advies nr. 73.442/2 van 7 juni 2023 wordt die bevoegdheid van de Koning behouden. Zoals reeds vermeld in het kader van de parlementaire werkzaamheden van de wet van 27 april 2016 inzake aanvullende maatregelen ter bestrijding van terrorisme is het noodzakelijk om een bepaalde souplesse te behouden om te kunnen reageren op rechtspraak van nationale of internationale controleoverheden (DOC 54 1727/001, blz. 25-26). Bovendien geeft deze bepaling de nodige flexibiliteit voor een aanpassing van de aanvullende nadere regels voor het beheer van de gemeenschappelijke gegevensbank omwille van de technologische ontwikkelingen die in dit stadium niet kunnen worden voorspeld.

Afdeling 4

Beheerder en operationeel verantwoordelijke

Zoals nu het geval is, worden er twee andere sleutelfuncties gecreëerd die specifiek zijn voor de gemeenschappelijke gegevensbank T.E.R.: de beheerder en de operationeel verantwoordelijke.

Voor een gegevensbank die door een veelvoud aan partners gevoed en geraadpleegd wordt bleek het belangrijk te voorzien in sleutelfuncties met specifieke opdrachten om de dagelijkse goede werking van de gegevensbank te verzekeren.

Er moet worden opgemerkt dat in navolging van advies 73.442/2 van 7 juni 2023 van de Raad van State wat de bevoegdheden van de Koning betreft, het artikel dat de Koning machtigde om de specifieke opdrachten van de beheerder en operationeel verantwoordelijke te bepalen, werd geschrapt.

Art. 11

Artikel 11 heeft betrekking op de beheerder van de gemeenschappelijke gegevensbank en zijn opdrachten. Om alle opdrachten van de beheerder in één enkele wettekst samen te brengen, wordt in dit artikel met betrekking tot zijn opdrachten niet alleen de inhoud van artikel 44/11/3bis, § 9, van de wet op het politieambt overgenomen, maar ook die van artikel 3 van het koninklijk besluit "TF" en van het koninklijk besluit "HP". De volgorde van de opdrachten werd ook herzien met

gestionnaire est désigné par le Roi sur proposition des ministres de la Justice et de l'Intérieur.

Sont ainsi reprises de l'arrêté royal "TF" et de l'arrêté royal "PH", la mission relative à l'établissement d'une liste des utilisateurs ce qui facilite sa mission générale en matière d'accès à la banque de données commune T.E.R ou encore celle relative à la traçabilité des traitements effectués dans la banque de données commune T.E.R.

Deux missions du gestionnaire ne sont toutefois plus reprises ici. Il s'agit des missions suivantes:

1) gérer et traiter les rapportages des incidents de sécurité tant sur le plan technique que fonctionnel;

2) informer dans les plus brefs délais le responsable opérationnel, le délégué à la protection des données et les autorités de contrôle de tout incident de sécurité constaté personnellement ou rapporté.

En effet, une disposition particulière, l'article 13, traite spécifiquement de la question de la gestion des brèches de sécurité. Il est renvoyé à cet article pour les explications complémentaires.

À l'article 11, 7°, le terme "service" a été ajouté afin d'envisager tous les cas de figure qui se présentent sur le terrain. Comme expliqué précédemment à l'article 8, il existe des services opérationnels, comme les services de renseignement, qui disposent d'un code d'identification unique pour l'ensemble des services dans les banques de données externes.

Art. 12

L'article 12 concerne le responsable opérationnel de la banque de données commune ainsi que ses missions. Il reprend le contenu de l'article 44/11/3bis, § 10, de la loi sur la fonction de police ainsi que l'article 4 de l'arrêté royal "TF" et de l'arrêté royal "PH" pour ce qui concerne ses missions. Outre les missions décrites à l'article 44/11/bis, § 10, de la loi sur la fonction de police, sont ajoutées ici, deux des missions du responsable opérationnel qui figuraient à l'article 4 de l'arrêté royal "TF" et de l'arrêté royal "PH".

La première mission ajoutée concerne la validation du statut d'une entité. Sur base des données et informations

het oog op de coherentie. De Koning wijst de beheerder aan op voordracht van de minister van Binnenlandse Zaken en de minister van Justitie.

De opdracht betreffende het opstellen van een lijst van de gebruikers, hetgeen de algemene opdracht van de beheerder inzake de toegang tot de gemeenschappelijke gegevensbank T.E.R. vergemakkelijkt of de opdracht betreffende de traceerbaarheid van de in de gemeenschappelijke gegevensbank T.E.R. uitgevoerde verwerkingen, zijn aldus ontleend aan de koninklijke besluiten "TF" en "HP".

Twee opdrachten van de beheerder zijn hier echter niet langer opgenomen. Het betreft de volgende opdrachten:

1) het zowel op technisch als op functioneel vlak beheren en behandelen van de rapportering van de veiligheidsincidenten;

2) het zo snel mogelijk, ter kennis brengen van elk veiligheidsincident dat persoonlijk vastgesteld wordt of gerapporteerd wordt, aan de operationeel verantwoordelijke, aan de functionaris voor gegevensbescherming en aan de toezichthoudende overheden.

Er is immers een bijzondere bepaling, artikel 13, die specifiek gaat over het beheer van de inbreuken op de beveiliging. Er wordt naar dit artikel verwezen voor verdere toelichting.

De term "diensten" werd aan artikel 11, 7°, toegevoegd om rekening te houden met alle gevallen die zich in het veld voordoen. Zoals voorheen uitgelegd bij artikel 8 zijn er dus operationele diensten, zoals de inlichtingendiensten, die beschikken over een unieke identificatiecode voor alle diensten in de externe gegevensbanken.

Art. 12

Artikel 12 heeft betrekking op de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank en zijn opdrachten. Het neemt met betrekking tot opdrachten de inhoud van artikel 44/11/3bis, § 10, van de wet op het politieambt over, alsook die van artikel 4 van het koninklijk besluit "TF" en het koninklijk besluit "HP". Naast de opdrachten omschreven in artikel 44/11/3bis, § 10, van de wet op het politieambt worden hier twee van de opdrachten van de operationeel verantwoordelijke die worden vermeld in artikel 4 van het koninklijk besluit "TF" en van het koninklijk besluit "HP" eraan toegevoegd.

De eerste toegevoegde opdracht betreft het valideren van het statuut van een entiteit. Op basis van de aan

transmises dans la banque de données commune T.E.R., le responsable opérationnel confirmera ou non si une personne physique majeure ou mineure de douze ans et plus, une personne morale ou une association de fait ainsi que l'ensemble des moyens utilisés par celles-ci, dès lors qu'elle répond aux critères d'un *foreign terrorist fighter*, *homegrown terrorist fighter*, extrémiste potentiellement violent, d'une personne condamnée pour terrorisme ou d'un propagandiste de haine doit être enregistrée dans la banque de données commune T.E.R. Cette validation par le responsable opérationnel confirmera la nécessité d'opérer un suivi de l'entité. La méthodologie utilisée par le responsable opérationnel pour la validation du statut d'une entité est intégrée dans la banque de données commune T.E.R. Le niveau de menace que représente l'entité ne détermine pas son statut. Il s'agit d'un élément parmi d'autres et c'est l'ensemble de ces éléments qui sera pris en compte pour valider ou non l'entité dans la banque de données commune T.E.R. Le Roi déterminera les modalités de cette validation.

La deuxième mission issue de l'arrêté royal "TF" et l'arrêté royal "PH" vise la qualité des données et informations transmises à la banque de données commune T.E.R. Dans le cadre d'une saine collaboration, le responsable opérationnel informera, le cas échéant, le service fournisseur si le responsable opérationnel décide que la donnée ou l'information concernée ne doit plus être enregistrée au niveau de la banque de données.

Enfin, la mission d'évaluation des données de la fiche de renseignements prévue à l'article 4 de des arrêtés royaux "TF" et "PH" n'est pas reprise dans la loi. En effet, actuellement, ces arrêtés désignent l'OCAM en tant que responsable opérationnel de la banque de données commune. La mission d'évaluation des données de la fiche de renseignement est une mission de l'OCAM en tant qu'Organe de coordination pour l'analyse de la menace. Si le rôle de responsable opérationnel devait être assuré par une autre autorité à l'avenir, cette tâche n'apparaîtrait plus.

Le point 3° a été reformulé en y ajoutant les termes "services de base" et ce, dans un souci de cohérence mais aussi pour viser le gestionnaire.

Notons qu'au travers des missions reprises aux points 2° et 3°, le responsable opérationnel apportera notamment son soutien aux différents services partenaires pour stimuler leur alimentation de la banque de données commune T.E.R.

de gemeenschappelijke gegevensbank T.E.R. doorgezonden gegevens en informatie, zal de operationeel verantwoordelijke bevestigen of een meerderjarige natuurlijke persoon of minderjarige natuurlijke persoon van twaalf jaar en ouder, een rechtspersoon of feitelijke vereniging, alsook alle de door hen aangewende middelen, indien zij voldoen aan de criteria van een *foreign terrorist fighter*, *homegrown terrorist fighter*, potentieel gewelddadige extremist, terrorismeveroordeelde of haatpropagandist al dan niet moet worden geregistreerd in de gemeenschappelijke gegevensbank T.E.R. Deze bekrachtiging door de operationeel verantwoordelijke zal de noodzaak bevestigen om de entiteit op te volgen. De door de operationeel verantwoordelijke gebruikte methode ter validatie van het statuut van een entiteit wordt opgenomen in de gemeenschappelijke gegevensbank T.E.R. Het dreigingsniveau dat de entiteit vormt bepaalt niet haar statuut. Het is één van de vele elementen en het zijn al die elementen waarmee rekening zal worden gehouden om de entiteit al dan niet te bekrachtigen in de gemeenschappelijke gegevensbank T.E.R. De Koning bepaalt de modaliteiten voor deze validatie.

De tweede opdracht die voortvloeit uit het koninklijk besluit "TF" en het koninklijk besluit "HP" betreft de kwaliteit van de gegevens en de informatie die naar de gemeenschappelijke gegevensbank T.E.R. doorgezonden worden. In het kader van een gezonde samenwerking, zal de operationeel verantwoordelijke, in voorkomend geval, de aanleverende dienst in kennis stellen wanneer het van oordeel is dat het gegeven of de informatie niet langer op het niveau van de gegevensbank geregistreerd moet blijven.

Ten slotte is de opdracht van evaluatie van de gegevens van de inlichtingenfiches bedoeld in artikel 4 van de koninklijke besluiten "TF" en "HP" niet opgenomen in de wet. Deze koninklijke besluiten wijzen thans immers het OCAD aan als operationeel verantwoordelijke van de gemeenschappelijke gegevensbank. De opdracht van de evaluatie van de gegevens van de inlichtingenfiche is een opdracht van het OCAD als Coördinatieorgaan voor de dreigingsanalyse. Indien de rol van operationeel verantwoordelijke in de toekomst moest worden verzekerd door een andere autoriteit, zou deze taak niet meer verschijnen.

Punt 3° werd geherformuleerd met toevoeging van de bewoordingen "basisdiensten" ten behoeve van de coherentie maar ook om de beheerder te beogen.

Er wordt op gewezen dat de operationeel verantwoordelijke door middel van de in de punten 2 en 3 genoemde opdrachten steun zal verlenen aan de verschillende partnerdiensten om hen aan te moedigen de gemeenschappelijke gegevensbank T.E.R. te voeden.

Au point 6°, les termes “l’Organe pour la coordination de l’analyse de la menace” ont été remplacés par les mots “le responsable opérationnel” car c’est en cette qualité que l’OCAM informe le service qui alimente la banque de données commune que la donnée transmise ne remplit pas ou plus un caractère adéquat, pertinent et non excessif au regard des missions visées à l’article 3, et des finalités visées à l’article 5, alinéa 2, et conclut que celle-ci doit dès lors être supprimée de la banque de données commune. Cette mission d’information est propre au responsable opérationnel, peu importe quel service est déterminé par le Roi pour assurer ce rôle.

À noter que la fonction de point de contact pour le responsable du traitement en matière de brèches de sécurité n’est également plus reprise ici mais bien dans la disposition spécifique de l’article 13 traitant des brèches de sécurité.

Art. 13

L’actuel article 44/11/3bis/, § 9, alinéa 2, 8° tiret, de la loi sur la fonction de police attribue au gestionnaire, à savoir, la police fédérale, la gestion et le rapportage des incidents de sécurité tant sur le plan technique que fonctionnel. L’article 3, 3° tiret de l’arrêté royal “TF” et l’article 3, 3°, de l’arrêté royal “PH” prévoient ainsi que la police fédérale informe dans les plus brefs délais le responsable opérationnel, le délégué à la protection des données, l’Organe et le Comité visés à l’article 44/11/3quinquies/2 de la loi sur la fonction de police de tout incident de sécurité constaté personnellement ou rapporté.

Cependant, il existe actuellement des lacunes dans la gestion et le traitement des incidents de sécurité dans la mesure où notamment, les incidents autres que de nature technique ou fonctionnelle ne sont pas réglés par la loi.

Par conséquent le nouvel article 13 entend:

1) mieux circonscrire la notion d’incident de sécurité. Les textes actuels utilisent en effet différents termes comme “incidents de sécurité” ou “manquements ou erreurs constatés”. Pour éviter toute confusion dans la terminologie utilisée, le projet opte pour la notion de “brèche de sécurité” telle que définie par l’article 26, 11° de la loi protection des données;

2) recentrer l’obligation de notification aux autorités de contrôle à ce qui est vraiment nécessaire. Par analogie aux articles 61, 89 et 155 de la loi sur la protection des

In punt 6° werden de bewoordingen “het Coördinatie-orgaan voor de dreigingsanalyse” vervangen door de woorden “de operationeel verantwoordelijke”, vermits het OCAD in die hoedanigheid de dienst die de gemeenschappelijke gegevensbank voedt ervan in kennis stelt dat het doorgegeven gegeven niet of niet langer toereikend, ter zake dienend of niet overmatig is in het licht van de opdrachten bedoeld in artikel 3, en ten opzichte van de doeleinden bedoeld in artikel 5, tweede lid, en besluit dat dit gegeven dus geschrapt moet worden uit de gemeenschappelijke gegevensbank. Die informatie is eigen aan de operationeel verantwoordelijke, ongeacht welke dienst de Koning aanwijst om die rol te verzekeren.

Er moet worden opgemerkt dat de rol van contactpunt voor de verwerkingsverantwoordelijke in het kader van inbreuken op de beveiliging hier ook niet langer is opgenomen, maar wel in de specifieke bepaling van artikel 13 betreffende de inbreuken op de beveiliging.

Art. 13

Huidig artikel 44/11/3bis, § 9, tweede lid, achtste streepje, van de wet op het politieambt kent het beheer en de rapportering van de veiligheidsincidenten toe aan de beheerder, namelijk de federale politie, zowel op technisch als op functioneel vlak. Artikel 3, derde streepje, van het koninklijk besluit “TF” en artikel 3, 3°, van het koninklijk besluit “HP” bepalen zo dat de federale politie zo snel mogelijk de operationeel verantwoordelijke, de functionaris voor gegevensbescherming, het Orgaan en het Comité bedoeld in artikel 44/11/3quinquies/2 van de wet op het politieambt in kennis stelt van elk veiligheidsincident dat persoonlijk wordt vastgesteld of wordt gerapporteerd.

Er bestaan nu echter lacunes in het beheer en de behandeling van veiligheidsincidenten, aangezien andere incidenten dan die van technische of functionele aard niet bij wet worden geregeld.

Het nieuwe artikel 13 bijgevolg beoogt:

1) een betere afbakening van het begrip “veiligheidsincident”. De huidige teksten gebruiken immers verschillende bewoordingen zoals “veiligheidsincidenten” of “gebreken of fouten die [...] vastgesteld worden”. Om enige verwarring over de gebruikte terminologie te voorkomen, kiest het ontwerp voor het begrip “inbreuk op de beveiliging” zoals bepaald in artikel 26, 11°, van de wet gegevensbescherming;

2) de toespitsing van de verplichte melding aan de toezichhoudende autoriteiten op wat echt noodzakelijk is. Naar analogie van de artikelen 61, 89 en 155 van de

données, le paragraphe 2 nouveau prévoit désormais que seules les brèches de sécurité susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques sont notifiées par le responsable opérationnel aux autorités de contrôle dans les meilleurs délais. Conformément à l'avis 73.442/2 du Conseil d'État du 7 juin 2023, la précision selon laquelle cette notification doit être faite "si possible 72 heures après que le responsable opérationnel en ait eu connaissance" est omise;

3) mieux définir les responsabilités du gestionnaire et du responsable opérationnel (ou ce qui est attendu d'eux);

4) créer un "single point of contact" pour tous les intervenants en matière d'incident de sécurité.

Par rapport aux points 3) et 4), comme expliqué ci-dessus, le nouvel article 13 prévoit désormais que la gestion et le rapportage de l'ensemble des brèches de sécurité relève des missions du responsable opérationnel.

En cas de survenance d'une brèche de sécurité, c'est le responsable opérationnel qui a le rôle principal. En effet, une brèche de sécurité ne se limite pas toujours à un problème technique. C'est un évènement plus large qui peut toucher l'efficacité de l'outil que constitue la banque de données commune T.E.R. Il peut s'agir de la diffusion inappropriée et non autorisée des données de la banque de données commune T.E.R., de la mauvaise qualité des données introduites dans la banque de données commune T.E.R. (art. 12, 1^o du projet). C'est aussi le responsable opérationnel qui est chargé de veiller à une exploitation des données conforme aux finalités de la banque de données commune T.E.R. (art. 12, 4^o du projet) ou encore d'informer un service qu'une des données qu'il a introduites n'est plus pertinente (art. 12, 6^o du projet) et qu'elle doit être supprimée. À ce niveau, ce n'est donc pas au gestionnaire de gérer ces problèmes mais au responsable opérationnel.

Néanmoins pour les brèches de nature technique et fonctionnelle, le gestionnaire est le mieux placé pour réagir adéquatement à un signalement de brèches et se faire communiquer l'ensemble des informations nécessaires pour identifier et comprendre une brèche de nature technique et fonctionnelle. C'est pour cette raison que la loi prévoit une collaboration entre le responsable opérationnel et le gestionnaire pour les brèches de sécurité qui sont de nature technique et fonctionnelle.

wet gegevensbescherming, bepaalt de nieuwe paragraaf 2 voortaan dat enkel inbreuken op de beveiliging die een hoog risico voor de rechten en vrijheden van natuurlijke personen inhouden door de operationeel verantwoordelijke zo snel mogelijk worden gemeld aan de toezichthoudende overheden. Overeenkomstig advies 73.442/2 van de Raad van State van 7 juni 2023 wordt de verduidelijking dat die melding "indien mogelijk, 72 uur nadat hij er kennis van heeft genomen" moet gebeuren, weggelaten;

3) een betere omschrijving van de verantwoordelijkheden van de beheerder en van de operationeel verantwoordelijke (of wat van hen wordt verwacht);

4) de oprichting van een "single point of contact" voor alle actoren in het kader van veiligheidsincidenten.

Met betrekking tot punten 3) en 4) bepaalt het nieuwe artikel 13, zoals hierboven werd uitgelegd, voortaan dat het beheer en de rapportering van alle inbreuken op de beveiliging onder de opdrachten van de operationeel verantwoordelijke vallen.

Indien er zich een inbreuk op de beveiliging voordoet, heeft de operationeel verantwoordelijke de belangrijkste rol. Een inbreuk op de beveiliging beperkt zich immers niet altijd tot een technisch probleem. Het is een ruimer gegeven dat kan raken aan de doeltreffendheid van de gemeenschappelijke gegevensbank T.E.R. als instrument. Het kan gaan om de ongepaste en ongeoorloofde verspreiding van de gegevens van de gemeenschappelijke gegevensbank T.E.R., de slechte kwaliteit van de gegevens die in de gemeenschappelijke gegevensbank T.E.R. zijn ingevoerd (art. 12, 1^o, van het ontwerp). Het is ook de operationeel verantwoordelijke die erop moet toezien dat de exploitatie van de gegevens beantwoordt aan de doeleinden van de gemeenschappelijke gegevensbank T.E.R. (art. 12, 4^o, van het ontwerp) of dat een dienst ervan in kennis gesteld wordt dat een van de gegevens die door de dienst is ingevoerd niet langer ter zake dienend is (art. 12, 6^o, van het ontwerp) en moet worden geschrapt. Op dat vlak is het dus niet aan de beheerder om die problemen aan te pakken, maar aan de operationeel verantwoordelijke.

Voor inbreuken van technische en functionele aard is de beheerder evenwel het best geplaatst om adequaat te reageren op een melding van inbreuken en om zich alle nodige informatie te laten meedelen om een inbreuk van technische en functionele aard te identificeren en te begrijpen. Daarom voorziet de wet in een samenwerking tussen de operationeel verantwoordelijke en de beheerder voor de inbreuken op de beveiliging die van technische en functionele aard zijn.

Suivant cette logique, le responsable opérationnel se voit désormais attribué le rôle d'informer le gestionnaire et le délégué à la protection des données de toute brèche de sécurité. Et, il reste le point de contact pour le responsable du traitement visé à l'article 5, alinéa 1^{er}, et l'informe des éventuelles brèches de sécurité, rôle qui lui est attribué actuellement par l'article 4, alinéa 1^{er}, 3^e tiret, de l'AR "TF" et l'article 4, alinéa 1^{er}, 3^e, de l'AR "PH." Pour rappel, le ministre de l'Intérieur et le ministre de la Justice sont responsables du traitement de la banque de données commune T.E.R. et exercent à ce titre une responsabilité sur la qualité des données et informations de la banque de données ainsi que sur le plan de la sécurité. Afin d'assurer ces responsabilités en connaissance de cause, le responsable du traitement pourra s'informer auprès du responsable opérationnel.

Dans son avis 73.442/2 du 7 juin 2023, le Conseil d'État demande d'harmoniser les paragraphes 2 et 3 en ce qui concerne "l'information" ou "la notification". Le paragraphe 3 est ainsi adapté pour se référer uniquement à la notification visée à l'alinéa 3, du paragraphe 2. En effet, le responsable opérationnel et le gestionnaire s'informent en permanence sur tous les types de brèche de sécurité (qu'ils soient graves ou non). Il s'agit d'un dialogue constant. Le responsable opérationnel en informe également le délégué la protection des données et le responsable du traitement. En revanche, dans les cas les plus graves, c'est-à-dire lorsque les brèches de sécurité sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physique, une notification, et non plus une simple information, est en plus nécessaire vis-à-vis des autorités de contrôle.

Enfin, l'article 13 prévoit certaines dispositions concernant le contenu de la notification. Cette notification doit désormais contenir au moins les informations suivantes:

1° la nature de la brèche de sécurité y compris, si possible, le nombre estimé de personnes et d'enregistrements de données à caractère personnel concernés;

2° le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

Volgens die logica wordt de operationeel verantwoordelijke thans de rol toegekend om de beheerder en de functionaris voor gegevensbescherming op de hoogte te brengen van elke inbreuk op de beveiliging. Hij blijft daarnaast het contactpunt voor de verwerkingsverantwoordelijke bedoeld in artikel 5, eerste lid, en stelt hem in kennis van eventuele inbreuken op de beveiliging, een rol die hem thans wordt toegekend bij artikel 4, eerste lid, derde streepje, van het koninklijk besluit "TF" en artikel 4, eerste lid, 3°, van het koninklijk besluit "HP". Ter herinnering, de ministers van Binnenlandse Zaken en van Justitie zijn verantwoordelijk voor de verwerking van de gemeenschappelijk gegevensbank T.E.R. en oefenen in die hoedanigheid een verantwoordelijkheid uit voor de kwaliteit van de gegevens en informatie van de gegevensbank alsook een verantwoordelijkheid op het niveau van de beveiliging. Om deze verantwoordelijkheden met kennis van zaken te kunnen uitoefenen, kan de verwerkingsverantwoordelijke zich informeren bij de operationeel verantwoordelijke.

De Raad van State verzoekt in advies 73.442/2 van 7 juni 2023 om het tweede en derde lid met elkaar in overeenstemming te brengen voor wat de begrippen "in kennis stellen" en "melding" betreft. Daarom wordt paragraaf 3 aangepast om enkel te verwijzen naar de in paragraaf 2, derde lid, bedoelde melding. De operationeel verantwoordelijke en de beheerder stellen zich namelijk continu op de hoogte van alle typen inbreuken op de beveiliging (ongeacht of ze al dan niet ernstig zijn). Het gaat om een constante dialoog. De operationeel verantwoordelijke stelt ook de functionaris voor gegevensbescherming en de verwerkingsverantwoordelijke ervan in kennis. In de ernstigste gevallen, met andere woorden in geval van een inbreuk op de beveiliging die aanleiding kan vormen tot een hoog risico voor de rechten en vrijheden van natuurlijke personen, moeten de toezichthoudende overheden daarentegen niet alleen eenvoudigweg in kennis worden gesteld, maar moeten ze ook een melding ontvangen.

Ten slotte bevat artikel 13 een aantal bepalingen betreffende de inhoud van de meldingen. Die meldingen moeten voortaan ten minste de volgende informatie bevatten:

1° de aard van de inbreuk op de beveiliging en indien mogelijk, bij benadering, het aantal betrokkenen en het aantal opnamen van persoonsgegevens waarover het gaat;

2° de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt bij wie bijkomende informatie kan worden verkregen;

3° les conséquences probables de la brèche de sécurité;

4° les mesures que le responsable opérationnel a prises ou propose de prendre pour remédier à la brèche de sécurité, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Ici aussi, le contenu de la notification reprend ce qui est prévu par les articles 61, 89 et 155 de la loi sur la protection des données.

Dans son avis du 13 juillet 2023, le Comité R indique que cet article contient des règles dérogatoires aux règles de l'article 155 de la loi relative à la protection des données et recommande de prévoir le cas particulier de la B.D.C. T.E.R. directement dans cette loi (§ 5). Toutefois, comme cela est expliqué dans l'introduction générale du chapitre 4 de l'avant-projet de loi, la loi relative à la protection des données reprend le régime général (et ordinaire) applicable aux traitements de données de la banque de données commune T.E.R. Les dispositions dérogatoires sont reprises dans l'avant-projet de loi pour pouvoir mieux prendre en compte la gestion spécifique de la banque de données entre responsables du traitement, gestionnaire et responsable opérationnel. Le gestionnaire et le responsable opérationnel ne sont en effet pas assimilables aux responsables du traitement et ne disposent pas de tous les attributs d'un préposé.

Section 5

Droits d'accès

dans la banque de données commune T.E.R.

Par rapport à la situation actuelle, cette section adapte le mécanisme d'accès à la banque de données commune. Actuellement, une gradation est prévue dans les accès aux données à caractère personnel et aux informations contenues dans les banques de données communes. Il s'agit de l'accès direct à l'ensemble des données et des entités ou à une partie de celles-ci, d'une part et de l'accès par le biais de l'interrogation directe sous forme de "hit no hit (l'entité existe: hit ou l'entité n'existe pas: no hit) d'autre part. Cette gradation suivait les dispositions de la loi sur la fonction de police en ce qui concerne l'accès à la banque de données nationale générale (BNG) mais n'est plus adaptée à la banque de données commune existante et visée par le présent projet. Une gradation est toujours prévue mais elle s'articule autour de différents droits d'utilisateurs: le droit de création, le droit de lecture, qui va de pair avec le droit/l'obligation d'écriture et, enfin, le droit

3° de waarschijnlijke gevolgen van de inbreuk op de beveiliging;

4° de maatregelen die de operationeel verantwoordelijke heeft genomen of voorgesteld om de inbreuk op de beveiliging aan te pakken, waaronder desgevallend maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Ook hier herneemt de inhoud van de melding wat is bepaald in de artikelen 61, 89 en 155 van de wet gegevensbescherming.

In het advies van 13 juli 2023 geeft Comité I aan dat dit artikel regels bevat die afwijken van de regels van artikel 155 van de wet gegevensbescherming en beveelt het aan dat het specifieke geval van de GGB T.E.R. rechtstreeks in die wet wordt geregeld (§ 5). Zoals nader verklaard in de algemene inleiding van hoofdstuk 4 van het voorontwerp van wet, behelst de wet gegevensbescherming evenwel de algemene (en gewone) regeling die van toepassing is op de gegevensverwerkingen in de gemeenschappelijke gegevensbank T.E.R. De afwijkende bepalingen worden overgenomen in het voorontwerp van wet teneinde beter rekening te houden met het specifieke beheer van de gegevensbank tussen de verwerkingsverantwoordelijken, de beheerder en de operationeel verantwoordelijke. De beheerder en de operationeel verantwoordelijke kunnen namelijk niet gelijk worden gesteld met verwerkingsverantwoordelijken en bezitten niet alle kenmerken van een aangestelde.

Afdeling 5

Toegangsrechten

in de gemeenschappelijke gegevensbank T.E.R.

Deze afdeling past het toegangsmechanisme tot de gemeenschappelijke gegevensbank aan ten opzichte van de huidige situatie. Thans is voorzien in een gradatie in de toegang tot de persoonsgegevens en informatie in de gemeenschappelijke gegevensbanken. Er bestaat enerzijds rechtstreekse toegang tot alle gegevens en entiteiten of tot een deel ervan en anderzijds, toegang via een rechtstreekse bevraging in de vorm van hit, no hit (de entiteit bestaat: hit – de entiteit bestaat niet: no hit). Die gradatie volgde de bepalingen van de wet op het politieambt voor wat de toegang tot de Algemene Nationale Gegevensbank (ANG) betreft, maar is niet nog aangepast aan de bestaande en door dit ontwerp beoogde gemeenschappelijke gegevensbank. Er wordt nog steeds voorzien in een gradatie, maar die is gebaseerd op verschillende toegangsrechten: het creatierecht, het leesrecht, dat samengaat met het schrijfrecht/de schrijfplicht en, tot slot, het vraagrecht. Deze gradatie wordt

d'interrogation. Cette gradation s'applique en fonction du type de partenaires ou services concernés et de leurs missions légales. Il faut noter que les différents services de base et services partenaire disposent des différents droits sur la base du respect des principes d'adéquation, de pertinence et du caractère non excessif (et donc sur base du principe du besoin d'en connaître) dans le cadre de l'exercice de leurs missions visées à l'article 3 et conformément aux finalités de l'article 5, alinéa 2. Ainsi, chaque service n'utilise ses droits dans la banque de données commune T.E.R. que dans le cadre de ses missions légales.

Les articles 14 à 16 reprennent le contenu de l'article 44/11/3^{ter}, §§ 1^{er} à 3, de la loi sur la fonction de police mais ont fait l'objet d'une reformulation en vue de les rendre plus lisibles et y intégrer les notions créées dans le projet, à savoir les différents droits énoncés au paragraphe ci-dessus et définis à l'article 2, 18° à 21°.

Les articles 14 à 16 visent successivement les services de base, les autorités de contrôle et les services partenaires en précisant le type de droit accordé à chacun d'eux.

Enfin, étant donné la définition des "autorités de contrôle" à l'article 2, 22°, les termes "l'Organe et le comité visés à l'article 44/11/3^{quinq}uies/2 de la loi sur la fonction de police" sont à chaque fois remplacés par les mots "les autorités de contrôle".

Il faut rappeler que, comme cela est prévu actuellement par les arrêtés royaux "TF" et "PH", les membres des services de base et des services partenaires qui ont accès aux données à caractère personnel et aux informations de la banque de données commune doivent disposer d'une habilitation de sécurité au minimum "secret". Il convient cependant de préciser que les membres des centres d'information et de communication ou des dispatching locaux de la police intégrée, ayant une fonction de coordination, désignés par leur directeur ou chef de corps, peuvent accéder à la carte d'information des entités traitées dans la banque de données commune T.E.R. sans devoir disposer d'une habilitation de sécurité.

Pour rappel, les magistrats du Ministère public n'ont pas besoin d'habilitation de sécurité (cf. article 8 de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité). Les autres membres du ministère public (par exemple, les juristes ou le personnel administratif), en revanche, doivent être titulaires d'une habilitation de sécurité de niveau "secret". Le Collège des procureurs généraux désignera, dans une circulaire, les catégories de personnes au sein du ministère public qui doivent avoir accès à la banque de

toegepast naargelang van het type betrokken partners of diensten en hun wettelijke opdrachten. Er wordt op gewezen dat de verschillende basisdiensten en partnerdiensten beschikken over verschillende rechten op basis van de inachtneming van de principes van toereikendheid, relevantie en de niet-bovenmatige aard (en dus op basis van het principe van de behoefte om te kennen) in het kader van de uitoefening van hun opdrachten bedoeld in artikel 3 en overeenkomstig de doelstellingen van artikel 5, tweede lid. Elke dienst maakt van zijn rechten in de gemeenschappelijke gegevensbank T.E.R. aldus enkel gebruik in het kader van zijn wettelijke opdrachten.

Artikelen 14 tot en met 16 hernemen de inhoud van artikel 44/11/3^{ter}, §§ 1 tot en met 3, van de wet op het politieambt, maar zijn geherformuleerd om ze leesbaarder te maken en de in het ontwerp gecreëerde begrippen, namelijk de verschillende rechten die worden vermeld in de bovenstaande paragraaf en gedefinieerd in artikel 2, 18° tot en met 21°, erin op te nemen.

Artikelen 14 tot en met 16 verwijzen achtereenvolgens naar de basisdiensten, de toezichthoudende overheden en de partnerdiensten, en verduidelijken het type van recht dat aan ieder van hen wordt verleend.

Ten slotte, gelet op de definitie van "toezichthoudende overheden" in artikel 2, 22° worden de termen 'het Orgaan en het Comité bedoeld in artikel 44/11/3^{quinq}uies/2 van de wet op het politieambt' telkens vervangen door de woorden "de toezichthoudende overheden".

Er moet op gewezen worden dat, zoals nu is bepaald in de koninklijke besluiten "TF" en "HP" de leden van de basisdiensten en de partnerdiensten die toegang hebben tot de persoonsgegevens en de informatie van de gemeenschappelijke gegevensbank, minstens moeten beschikken over een veiligheidsmachtiging van het niveau "geheim". De leden van de informatie- en communicatiecentra of lokale dispatching van de geïntegreerde politie, met een coördinerende functie, aangewezen door hun directeur of korpschef, kunnen de informatiekaart van de in de gemeenschappelijke gegevensbank T.E.R. verwerkte entiteiten raadplegen zonder een veiligheidsmachtiging te moeten verkrijgen.

Ter herinnering, de magistraten van het Openbaar Ministerie hebben geen veiligheidsmachtiging nodig (cfr. artikel 8 van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen). De andere leden van het Openbaar Ministerie (bv juristen of administratief personeel) moeten daarentegen wel houder zijn van een veiligheidsmachtiging van het niveau "geheim". Het College van procureurs-generaal zal in een omzendbrief de categorieën van personen binnen het

données commune T.E.R., à condition qu'elles soient titulaires de l'habilitation de sécurité susmentionnée.

Art. 14

Comme cela est prévu à l'article 44/11/3^{ter}, § 1^{er}, alinéa 1^{er}, de la loi sur la fonction de police, l'article 14 prévoit un accès direct (nouveaux droit d'écriture et droit de lecture) pour les services de base qui sont les partenaires opérationnels incontournables en ce qui concerne la lutte contre le terrorisme: l'Organe de coordination pour l'analyse de la menace (OCAM), la police intégrée et les services de renseignement et de sécurité. Étant donné la définition des services de base à l'article 2, 2^o, ceux-ci ne sont plus énumérés dans le présent article.

Dans l'article 14, les services de base bénéficient désormais d'un droit de création, d'un droit de lecture et d'un droit d'écriture dans la banque de données commune.

En effet, seul un service de base peut créer une nouvelle entité dans la banque de données commune (cf. article 17), il s'agit du droit de création. Le droit de lecture leur permet de consulter tout ou partie des données à caractère personnel et des informations de la banque de données commune, tandis que le droit/l'obligation d'écriture leur permet d'introduire, de modifier ou d'effacer des données à caractère personnel et des informations relatives à une entité dans la banque de données commune.

Dans son avis du 13 juillet 2023, le Comité R estime que le "besoin d'en connaître" est un principe servant à éviter que des personnes non-autorisées prennent connaissance d'informations sensibles, et non une règle de protection des données (§ 7). Il faut d'abord préciser que le libellé du "besoin d'en connaître" a été remplacé par le "principe d'adéquation, de pertinence et du caractère non excessif" tel que prévu par la loi relative à la protection des données. Par ailleurs, le "need to know" est un principe essentiel en matière de protection des données dans la mesure où un responsable du traitement est tenu de vérifier que ceux qui ont accès à des données à caractère personnel n'en font pas un traitement abusif, *a contrario*, qu'ils ont le besoin d'en connaître. Il reprend ainsi le principe selon lequel l'accès aux données et les possibilités de traitement sont limités à ce dont les personnes ont besoin pour l'exercice de leurs fonctions, et donc à ce qui est utile à l'exercice de leurs fonctions, ou aux besoins du service, tels que prévu aux articles 14, § 4, al. 2, 1^o, 45, § 4, 1^o, 83, 2^o et 149, 2^o de la loi relative à la protection des données. On retrouve également ce vocabulaire dans

Openbaar Ministerie aanduiden die toegang nodig hebben tot de gemeenschappelijke gegevensbank T.E.R., mits zij beschikken over voormelde veiligheidsmachtiging.

Art. 14

Zoals bepaald in artikel 44/11/3^{ter}, § 1, eerste lid, van de wet op het politieambt, voorziet artikel 14 in een rechtstreekse toegang (nieuw leesrecht en schrijfrecht) voor de basisdiensten die de essentiële operationele partners in de strijd tegen het terrorisme zijn, met name het Coördinatieorgaan voor de dreigingsanalyse (OCAD), de geïntegreerde politie en de inlichtingen- en veiligheidsdiensten. Gelet op de definitie van de basisdiensten in artikel 2, 2^o, worden die diensten niet meer opgesomd in dit artikel.

Op basis van artikel 14 beschikken de basisdiensten voortaan over een creatierecht, een leesrecht en een schrijfrecht in de gemeenschappelijke gegevensbank.

Alleen een basisdienst kan immers een nieuwe entiteit creëren in de gemeenschappelijke gegevensbank (zie artikel 17), dit is het creatierecht. Op basis van het leesrecht kunnen de basisdiensten alle of een deel van de persoonsgegevens en informatie in de gemeenschappelijke gegevensbank raadplegen, terwijl het schrijfrecht/de schrijfplicht aan hen de mogelijkheid biedt persoonsgegevens en informatie met betrekking tot een entiteit in de gemeenschappelijke gegevensbank in te voeren, te wijzigen of te wissen.

In het advies van 13 juli 2023 is Comité I van mening dat de "need to know" een principe is dat wordt gebruikt om te voorkomen dat onbevoegden toegang krijgen tot gevoelige informatie, en geen regel voor gegevensbescherming (§ 7). Vooreerst dient te worden gepreciseerd dat de formulering "behoefte om te kennen" vervangen werd door 'het principe van toereikendheid, relevantie en de niet-bovenmatige aard' als bepaald door de wet gegevensbescherming. De "need to know" is overigens een kernprincipe in de context van gegevensbescherming, waarbij een verwerkingsverantwoordelijke moet nagaan of zij die toegang hebben tot persoonsgegevens daar geen misbruik van maken, *a contrario*, dat ze er kennis van moeten hebben. Hierbij wordt aldus het principe overgenomen dat stelt dat de toegang tot de gegevens en de verwerkingsmogelijkheden beperkt blijven tot dat wat men nodig heeft voor de uitoefening van zijn opdrachten en dus tot wat nuttig is voor de uitoefening van zijn opdrachten of voor de behoeften van de dienst zoals bedoeld in de artikelen 14, § 4, tweede lid, 1^o, 45, § 4, 1^o, 83, 2^o, en 149, 2^o. Dit concept kan men ook terugvinden in de wet op het politieambt (artikel 44/4, § 5,

la loi sur la fonction de police (art. 44/4, § 5, 1^o) mais aussi dans la loi du 10 juillet 2006 relative à l'analyse de la menace (art. 10, § 1^{er}, f), et § 3, al. 2, art. 11, al. 1^{er} et 2, art. 12, al. 1^{er} et 2).

Par ailleurs, comme le rappelle à juste titre le Comité R, "il ne suffit pas de disposer du "besoin d'en connaître" (non autrement caractérisé) pour qu'un traitement de données (tel qu'un accès à une entrée de la B.D.C. T.E.R.) remplisse les conditions visées aux articles 140 et 141 de la L.P.D. En d'autres termes, le "besoin d'en connaître" n'est pas et ne peut pas être un blanc-seing pour la consultation des données personnelles. Chaque traitement doit être évalué au cas par cas et la responsabilité ultime réside chez le responsable du traitement." (§ 7).

Art. 15

L'article 15, paragraphe 1^{er}, donne aux autorités de contrôle, uniquement, un droit de lecture dans la banque de données commun afin de leur permettre d'assurer leur mission de contrôle du traitement des données à caractère personnel dans cette banque de données commune.

L'article 44/11/3^{ter}, § 1^{er}, alinéa 2, de la loi sur la fonction de police leur octroyait un accès direct à la banque de données commune. Cela leur permettait non seulement de consulter tout ou partie des données à caractère personnel et des informations de la banque de données commune mais aussi d'y introduire des données et informations. Or, pour l'exercice de leur mission, cette deuxième possibilité n'est pas nécessaire. Raison pour laquelle, le projet ne leur octroie désormais plus qu'un droit de lecture sans droit d'écriture. On peut mentionner ici l'avis du Comité R du 13 juillet 2023 dans lequel il recommande donc qu'un droit de lecture incluant toutes les informations et données (y compris la fiche d'information) lui soit reconnu, de manière immédiate (pas d'intervention des gestionnaire ou responsable opérationnel nécessaire) (§ 16). Cela est déjà prévu.

Conformément à l'avis du Conseil d'État 73.442/2 du 7 juin 2023, il convient de mentionner que cet article constitue une exception au principe selon lequel le droit de lecture et le droit d'écriture vont de pair. Mais cela se justifie car les autorités de contrôle ne sont ni des services partenaires, ni des services de base. Elles ont besoin d'un accès dans la banque de données commune T.E.R. uniquement eu égard à leurs missions de contrôle et le droit de lecture est suffisant dans leur chef pour exercer ces missions.

1^o) en in de wet van 10 juli 2006 betreffende de analyse van de dreiging (artikelen 10, § 1, f), en § 3, tweede lid, 11, eerste en tweede lid, artikel 12, eerste en tweede lid).

Bovendien is het, zoals Comité I correct aanhaalt, "niet voldoende [...] om een "need to know" te hebben (niet anders gekarakteriseerd) opdat een gegevensverwerkende handeling (zoals de toegang tot een input van de GGB TER) zou voldoen aan de voorwaarden van de artikels 140 en 141 GBW. Met andere woorden, de "need to know" is geen blanco volmacht voor het raadplegen van persoonlijke gegevens en kan dat ook niet zijn. Elke verwerking moet per geval worden beoordeeld en de uiteindelijke verantwoordelijkheid ligt bij de persoon die verantwoordelijk is voor de verwerking." (§ 7).

Art. 15

Artikel 15, paragraaf 1, verleent de toezichthoudende overheden enkel een leesrecht in de gemeenschappelijke gegevensbank zodat deze hun opdracht inzake de controle op de verwerking van de persoonsgegevens in die gemeenschappelijke gegevensbank kunnen uitvoeren.

Artikel 44/11/3^{ter}, § 1, tweede lid, van de wet op het politieambt verleende hen een rechtstreekse toegang tot de gemeenschappelijke gegevensbank. Op basis daarvan konden ze niet alleen alle of een deel van de persoonsgegevens en informatie in de gemeenschappelijke gegevensbank raadplegen, maar ook gegevens en informatie invoeren. Voor de uitoefening van hun opdracht is die tweede mogelijkheid echter niet noodzakelijk. Om die reden verleent het ontwerp hen voortaan enkel nog een leesrecht zonder schrijfrecht. Hier kan het advies van Comité I van 13 juli 2023 worden aangehaald, waarin het aanbeveelt dat zij het recht krijgen om alle informatie en gegevens te lezen (met inbegrip van de informatiefiche), en zulks onmiddellijk (geen tussenkomst van de beheerder of operationele verantwoordelijke vereist) (§ 16). Daarin is reeds voorzien.

Overeenkomstig advies 73.442/2 van 7 juni 2023 van de Raad van State moet er worden vermeld dat dit artikel een uitzondering vormt op het principe dat het leesrecht altijd verbonden is aan het schrijfrecht. Dat is evenwel gerechtvaardigd omdat de toezichthoudende overheden noch partnerdiensten, noch basisdiensten zijn. Ze hebben enkel toegang nodig tot de gemeenschappelijke gegevensbank T.E.R. in het kader van hun toezichtsoptredens, en het leesrecht volstaat voor de uitoefening ervan.

De même, le paragraphe 2 de cet article octroie au Comité permanent de contrôle des services de police et son service enquêtes, uniquement, un droit de lecture dans la banque de données commun afin de leur permettre d'assurer leur mission de contrôle. Il s'agit ici aussi d'une exception au principe selon lequel le droit de lecture et le droit d'écriture vont de pair, pour les mêmes raisons que celles évoquées pour les autorités de contrôles.

Afin d'accomplir correctement ses missions légales, le Comité P et son Service d'enquêtes ont actuellement accès à différentes banques de données, dont le Registre national, la BNG, la DIV, le casier judiciaire central, etc. Ces accès répondent d'ailleurs également à la nécessité d'avoir accès à des sources de données authentiques.

Actuellement, le Comité permanent P n'a pas accès à la banque de données commune (BDC). L'accès du Comité permanent P et de son Service d'enquêtes ne se justifie pas par une nécessité de contrôler le fonctionnement de la BDC, mais bien par le fait que la police et l'OCAM y ont accès et que le Comité permanent P exerce un contrôle sur ces services, qui ont eux-mêmes accès à la BDC. La finalité est donc d'avoir une vue de la position d'information dont la police ou l'OCAM disposait ou aurait pu disposer à un moment donné lors d'une consultation de la BDC.

L'accès à la BDC est complémentaire par rapport aux accès déjà existants à la BNG et/ou au casier judiciaire.

Afin non seulement d'exécuter efficacement les missions que le législateur a confiées au Comité P et à son Service d'enquêtes, mais aussi de pouvoir garantir la confidentialité nécessaire à la protection de la vie privée voire, le cas échéant, d'accorder à des particuliers ou à des membres des services de police l'anonymat demandé, il est essentiel que le Comité P et son Service d'enquêtes puissent obtenir rapidement et directement toutes les données pertinentes utiles à cet effet sans devoir faire appel à d'autres services que le Comité P contrôle éventuellement lui-même.

En tant qu'organe indépendant et externe, le Comité P exerce un contrôle sur les membres des services de police et l'OCAM (y compris le Comité permanent R) qui ont déjà accès aux données de la BDC.

Conformément à l'article 16, alinéa 3, de la loi organique du 18 juillet 1991 "du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace", le Service d'enquêtes P effectue,

Evenzo krijgt het Vast Comité van Toezicht op de politiediensten en zijn Dienst Enquêtes in paragraaf 2 van dit artikel enkel een leesrecht in de gemeenschappelijke gegevensbank toegekend zodat ze hun toezichtsoverdracht kunnen uitoefenen. Dit is evenzeer een uitzondering op het principe dat het leesrecht altijd verbonden is aan het schrijfrecht, om dezelfde redenen als die welke zijn aangehaald voor de toezichthoudende overheden.

Om zijn wettelijke opdrachten naar behoren te kunnen vervullen beschikken het Comité P en zijn Dienst Enquêtes thans over een toegang tot verschillende databanken, waaronder het RRN, de ANG, de DIV, het centraal strafregister, ... Deze toegangen kaderen trouwens ook in de noodzaak om toegang te hebben tot authentieke gegevensbronnen.

Op dit ogenblik heeft het VCP geen toegang tot de gemeenschappelijke gegevensbank (GGB). De toegang voor het VCP en zijn dienst Enquêtes wordt niet gemotiveerd vanuit een toezicht op de werking van de GGB maar wel op basis van het feit dat de politie en het OCAD toegang hebben en het VCP controle uitoefent op deze diensten, die zelf toegang hebben tot de GGB. De finaliteit is dus om een zicht te hebben op de informatiepositie waarover de politie of het OCAD op een gegeven moment beschikte of had kunnen beschikken bij een consultatie van de GGB.

De toegang tot de GGB is complementair ten opzichte van de reeds bestaande toegangen tot de ANG en/of het strafregister.

Teneinde niet enkel op doeltreffende wijze de opdrachten uit te voeren die de wetgever het Comité P en zijn Dienst Enquêtes heeft toevertrouwd, maar ook om de vertrouwelijkheid, die noodzakelijk is ter bescherming van de persoonlijke levenssfeer en zelfs, in gebeurlijk geval, de gevraagde anonimiteit, te kunnen waarborgen, aan particulieren of leden van de politiediensten het van essentieel belang dat het Comité P en zijn Dienst Enquêtes snel en rechtstreeks kunnen beschikken over alle relevante gegevens die hiertoe nodig zijn zonder hierbij beroep te moeten doen op andere diensten die het mogelijks zelf controleert.

Het Comité P oefent als onafhankelijk en extern orgaan toezicht uit over leden van de politiediensten en het OCAD (met het VCI) die al toegang hebben tot de gegevens van de GGB.

Overeenkomstig artikel 16, 3de lid, van de organieke wet van 18 juli 1991 "tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse" stelt de Dienst Enquêtes P,

en concurrence avec les autres officiers et agents de police judiciaire et même avec un droit de priorité sur ces derniers, des enquêtes sur les crimes et délits mis à charge des membres des services de police et de l'OCAM. Lorsqu'il travaille en tant que service d'enquête spécialisé pour le compte des autorités judiciaires et qu'il constate, dans ce cadre, les infractions commises par les membres des services de police et de l'OCAM, le Service d'enquêtes P, sous l'autorité de ces autorités judiciaires, agit comme un service de police à part entière qui, au besoin, prend en filature des suspects, procède à des auditions, effectue les constatations nécessaires et accomplit les actes requis en matière de procédure pénale.

Partant, le Service d'enquêtes P doit nécessairement avoir accès à toutes les informations – y compris celles de la BDC – dont disposent également les services de police revêtus d'une compétence générale de police administrative et de police judiciaire.

Les motifs légitimant l'accès à la BDC pour la police intégrée en vue de l'exercice de ses missions judiciaires sont donc applicables *mutatis mutandis* à l'accès réservé au Service d'enquêtes P dans le cadre de ces missions. Il est également nécessaire que le Service d'enquêtes P ait accès à la BDC dans les cas où une intervention policière (p. ex. perquisition, arrestation) lui est confiée et qu'une analyse de risques préalable doit donc être réalisée.

Il est nécessaire que le Comité P (et son Service d'enquêtes), dans le cadre de sa fonction de contrôle prévue par la loi, ait également accès aux mêmes sources de données authentiques que celles auxquelles les membres de la police intégrée ont accès, telles que celles de la BDC. Un contrôle efficace et effectif n'est possible que si le Comité P (et son Service d'enquêtes) dispose exactement des mêmes accès, ce, par exemple, afin de pouvoir recommencer objectivement le processus de collecte d'informations de la police en cas d'enquête, sans devoir se baser uniquement sur ce que la "personne contrôlée" mentionne à cet égard. En outre, il ressort de l'expérience que le Comité permanent P a faite de la consultation des autres sources de données authentiques qu'une consultation directe de la BDC permettra parfois de ne pas solliciter outre mesure la police et d'éviter que la plainte soit considérée comme infondée ou sans objet.

En ce qui concerne le traitement de ses données à caractère personnel, le Comité P (et son Service d'enquêtes) est soumis aux règles contenues dans la loi relative à la protection des données.

samen met de andere officieren en agenten van gerechtelijke politie en zelfs met een recht van voorrang op deze laatste, de onderzoeken in naar de misdaden en wanbedrijven die ten laste worden gelegd van de leden van de politiediensten en van het OCAD. Wanneer de Dienst Enquêtes als een gespecialiseerde onderzoeksdienst voor rekening van de gerechtelijke overheden werkt, waarbij deze de door leden van de politiediensten en van het OCAD gepleegde strafbare feiten vaststelt, treedt de Dienst Enquêtes P, onder het gezag van die gerechtelijke overheden, op als een volwaardige politiedienst die zo nodig verdachten schaduwt en verhoren afneemt, de nodige waarnemingen doet en de vereiste handelingen inzake strafprocedure verricht.

Het is dus zo dat de Dienst Enquêtes P bijgevolg noodgedwongen toegang moet krijgen tot alle informatie – waaronder deze van de GGB – waarover de politiediensten met algemene bevoegdheid van bestuurlijke en gerechtelijke politie ook beschikken.

De motivering inzake toegang tot de GGB voor de geïntegreerde politie, voor de uitoefening van haar gerechtelijke opdrachten, is dus *mutatis mutandis* van toepassing op de toegang voor de Dienst Enquêtes P in het kader van deze opdrachten. De toegang tot de GGB voor de Dienst Enquêtes P is ook noodzakelijk in die gevallen waar een politionele interventie (bijvoorbeeld huiszoeking, arrestatie) hen opgedragen wordt en er dus een voorafgaandelijke risicoanalyse dient te worden opgemaakt.

Het is noodzakelijk dat het Comité P (en zijn Dienst Enquêtes), vanuit zijn wettelijk voorziene toezichtfunctie, ook toegang krijgt tot dezelfde authentieke gegevensbronnen als deze waar leden van de GPI toegang toe hebben; zoals deze tot de GGB. Een effectieve en efficiënte controle is maar mogelijk als het Comité P (en zijn Dienst Enquêtes) exact dezelfde toegangen heeft. Dit bijvoorbeeld om in geval van onderzoek op objectieve wijze het informatieverzamelingsproces van de politie te kunnen overdoen zonder zich hierbij enkel te moeten baseren op wat de "gecontroleerde" hierover meldt. De ervaring met consultatie van de andere authentieke gegevensbronnen heeft het Vast Comité P bovendien geleerd dat een onmiddellijke consultatie van de GGB er soms zal toe leiden dat de politie verder niet moet verontrust worden en de klacht ongegrond of zonder voorwerp is.

Het Comité P (en zijn Dienst Enquêtes) is wat betreft de verwerking van zijn persoonsgegevens onderworpen aan de regels die opgenomen werden in de Wet gegevensbescherming.

La loi du 18 juillet 1991 prévoit des mécanismes de contrôle et des garanties afin d'assurer la confidentialité et le secret des données.

— Elle contient des dispositions visant à préserver la confidentialité des dossiers et à protéger la vie privée des personnes lorsque des enquêtes, des rapports et des conclusions sont rendus publics.

— Il est prévu que les membres du personnel du Comité P sont tenus à une obligation de secret, qui subsiste lorsqu'ils ont cessé leurs fonctions.

— Le Comité P doit rendre compte à la Commission spéciale chargée de l'accompagnement parlementaire du Comité permanent de contrôle des services de police.

Enfin, le paragraphe 3 octroie à l'Inspection générale de la police fédérale et de la police locale, uniquement, un droit de lecture dans la banque de données commun afin de lui permettre d'assurer sa missions de contrôle qui lui est attribuée par l'article 5 de la loi du 15 mai 2007 "sur l'Inspection générale et portant des dispositions diverses relatives au statut de certains membres des services de police". Il s'agit ici aussi d'une exception au principe selon lequel le droit de lecture et le droit d'écriture vont de pair, pour les mêmes raisons que celles évoquées pour les autorités de contrôle. La motivation pour l'accès par le Comité P et son Service d'enquêtes à la banque de données commune vaut *mutatis mutandis* aussi pour l'AIG dans son rôle d'enquête et de contrôle des services de police.

Art. 16

Comme cela est prévu à l'article 44/11/3^{ter}, § 2, de la loi sur la fonction de police, l'article 17 prévoit différents types d'accès pour les services partenaires énumérés à l'article 1^{er}, 3°. Ceux-ci peuvent bénéficier, soit d'un droit de lecture et d'un droit d'écriture dans la banque de données commune, correspondant à l'actuel accès direct à la banque données commune T.E.R., soit d'un droit d'interrogation, correspondant à l'actuel interrogation directe dans la banque de données commune. Tout comme le système actuel de l'accès direct implique de consulter et d'alimenter la banque de données, les droits de lecture et d'écriture sont indissociables. Par conséquent, les services partenaires qui consultent la banque de données commune sur base du droit de lecture sont tenus également d'introduire des données sur base du droit/ de l'obligation d'écriture (art. 18 du projet). À noter que si, à la suite de l'exercice de son droit de lecture, un service partenaire doit prendre des

In de wet van 18 juli 1991 zijn controlemechanismen ingebouwd en waarborgen voorzien die de vertrouwelijkheid en de geheimhouding van de gegevens garanderen.

— Er zijn bepalingen opgenomen die erop gericht zijn om in geval van het openbaar maken van de onderzoeken, verslagen en besluiten de vertrouwelijkheid van de dossiers veilig te stellen en het privéleven van de personen te beschermen.

— Er is voorzien dat de personeelsleden van het Comité P gehouden zijn tot een geheimhoudingsplicht, die blijft bestaan na het beëindigen van de functie.

— Het Comité P dient verantwoording af te leggen aan de Bijzondere commissie belast met de parlementaire begeleiding van het Vast Comité van Toezicht op de politiediensten.

Tot slot krijgt de Algemene Inspectie van de federale politie en van de lokale politie in paragraaf 3 enkel een leesrecht in de gemeenschappelijke gegevensbank toegekend zodat ze haar toezichtsoopdrachten kan uitoefenen zoals bedoeld in artikel 5 van de wet van 15 mei 2007 op de Algemene Inspectie en houdende diverse bepalingen betreffende de rechtspositie van sommige leden van de politiediensten. Dit is ook een uitzondering op het principe dat het leesrecht altijd verbonden is aan het schrijfrecht, om dezelfde redenen als die welke zijn aangehaald voor de toezichthoudende overheden. De motivering voor het Comité P en zijn Dienst Enquêtes om toegang te hebben tot de gemeenschappelijke gegevensbank geldt *mutatis mutandis* ook voor de IAG in haar rol van onderzoeker en toezicht van de politiediensten.

Art. 16

Zoals bepaald in artikel 44/11/3^{ter}, § 2, van de wet op het politieambt, voorziet artikel 17 in verschillende types van toegang voor de in artikel 1, 3°, opgesomde partnerdiensten. Zij kunnen beschikken over ofwel een leesrecht en een schrijfrecht in de gemeenschappelijke gegevensbank, hetgeen overeenkomt met de huidige directe toegang tot de gemeenschappelijke gegevensbank T.E.R., ofwel een vraagrecht hetgeen overeenkomt met de huidige rechtstreekse bevraging in de gemeenschappelijke gegevensbank. Net zoals het huidige systeem van rechtstreekse toegang inhoudt dat de gegevensbank wordt geraadpleegd en gevoed, zijn de lees- en schrijfrechten onlosmakelijk met elkaar verbonden. Bijgevolg zijn de partnerdiensten die de gemeenschappelijke gegevensbank op basis van het leesrecht raadplegen, ook verplicht gegevens in te voeren op basis van het schrijfrecht/de schrijfplicht (artikel 18 van het ontwerp). Opgemerkt dient te worden dat indien

décisions administratives, il en informe un des services de base. À cet effet, un point de contact au sein de chaque service partenaire devra être désigné dans une circulaire ministérielle.

Ici également, le besoin d'en connaître vise la nécessité de prendre connaissance de données à caractère personnel et informations de la banque de données commune T.E.R. pour l'exercice de missions légales.

Par rapport à l'article 44/11/3ter, § 2, les termes "au niveau stratégique, tactique ou opérationnel" ne sont plus repris dans l'article 16. En effet, il ne s'agit que d'une finalité de la banque de données commune et ils n'apportaient aucune plus-value au texte étant donné l'énumération des finalités de la BDC reprises à l'article 5 et ne consistait qu'en une répétition inutile. De plus, étant donné la définition des services partenaires à l'article 2, 3°, ceux-ci ne sont plus énoncés dans le présent article. Par ailleurs, le besoin d'en connaître a été remplacé par le respect des principes d'adéquation, de pertinence et du caractère non excessif.

Le Roi déterminera par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, le type de droit d'accès et ses modalités dont bénéficie chaque service partenaire. Dans son avis du 20 juin 2023, le C.O.C. recommande de prévoir le type spécifique d'accès à la base de données commune T.E.R., ainsi que le cadre dans lequel le service partenaire concerné sera autorisé à exercer ces droits. Cependant, il appartient au Roi d'organiser ses services comme il l'entend. En outre, les missions du service partenaire concerné peuvent changer et impliquer un changement dans le type de droit d'accès qui doit lui être octroyé. Une certaine flexibilité est dès lors nécessaire.

Ainsi, comme précisé ci-avant, il a été décidé de reprendre le type de droit d'accès dont bénéficie chaque service partenaire dans la banque de données commune T.E.R. dans un arrêté royal plutôt que dans la loi pour conserver une certaine flexibilité dans l'octroi, le retrait ou la modification de l'accès en fonction de l'évolution des compétences, des missions et des besoins des différents services partenaires.

Il convient également de préciser que compte tenu de la position particulière et de l'indépendance du ministère public telles que prévues à l'article 151 de la Constitution, ainsi que la nécessité de pouvoir sauvegarder le secret de l'information, comme mentionné *supra*, l'arrêté royal relatif à l'interconnexion de ou vers les banques de données

een partnerdienst na de uitoefening van zijn leesrecht administratieve beslissingen moet nemen, het raadzaam is om een van de basisdiensten hiervan op de hoogte te stellen. Daartoe moet binnen elke partnerdienst een aanspreekpunt worden aangeduid in een ministeriële omzendbrief.

Ook hier verwijst de behoefte om te kennen naar de noodzaak om kennis te nemen van en informatie voor de uitoefening van wettelijke opdrachten.

Ten opzichte van artikel 44/11/3ter, § 2, zijn de termen 'op strategisch, tactisch of operationeel vlak' niet langer opgenomen in artikel 16. Het betreft namelijk slechts één doeleinde van de gemeenschappelijke gegevensbank en gelet op de opsomming van de doeleinden van de GGB in artikel 5 boden die termen geen enkele meerwaarde aan de tekst en vormden ze slechts een onnodige herhaling. Bovendien worden deze, gelet op de definitie van de partnerdiensten in artikel 2, 3°, niet meer vermeld in dit artikel. Overigens werd de behoefte om te kennen vervangen door de inachtneming van de principes van toereikendheid, relevantie en de niet-bovenmatige aard.

De Koning zal, bij een in Ministerraad overlegd besluit en na advies van de toezichthoudende overheden, het type van toegangsrecht en de nadere regels ervan voor elke partnerdienst bepalen. In het advies van 20 juni 2023 beveelt het COC aan om te voorzien in het specifieke type van toegang tot de gemeenschappelijke gegevensbank T.E.R., alsook in het kader waarin de betreffende partnerdienst die rechten zal mogen aanwenden. Het komt echter de Koning toe zijn diensten naar eigen goeddunken te organiseren. Bovendien kunnen de opdrachten van de betrokken partnerdienst veranderen, en dat kan betekenen dat het hem toegekende type toegangsrecht verandert. Bijgevolg is enige flexibiliteit vereist.

Aldus is er, zoals hierboven verduidelijkt, voor gekozen het type toegangsrecht dat elke partnerdienst in de gemeenschappelijke gegevensbank T.E.R. geniet, in een koninklijk besluit en niet in de wet op te nemen, teneinde een zekere flexibiliteit te behouden bij het verlenen, intrekken of wijzigen van de toegang naar gelang van de evolutie van de bevoegdheden, opdrachten en behoeften van de verschillende partnerdiensten.

Er wordt tevens op gewezen dat, gelet op de bijzondere positie en de onafhankelijkheid van het Openbaar Ministerie waarin het artikel 151 van de Grondwet voorziet en de noodzaak om het geheim van het opsporingsonderzoek te vrijwaren, zoals hoger reeds vermeld, het koninklijk besluit betreffende de koppeling van of naar

du Ministère public ne pourra être adopté qu' "après avis conforme du Collège des procureurs généraux".

Il est renvoyé au commentaire de l'article 14 en ce qui concerne l'avis du Comité R du 13 juillet 2023 relatif au "besoin d'en connaître" (§ 7).

Section 6

*Création d'une entité et alimentation
de la banque de données commune T.E.R.*

Art. 17

L'article 17 reprend le principe de l'article 9 de l'arrêté royal "TF" et de l'arrêté royal "PH" selon lequel seul un service de base peut créer et donc enregistrer une entité dans la banque de données commune (droit de création).

Il faut rappeler que les enregistrements dans la banque de données commune T.E.R. s'effectuent de manière objective. Il y a lieu de respecter des critères clairs, ancrés légalement, pour effectuer un enregistrement dans la banque de données commune T.E.R. N'importe quelle entité n'y figure pas, pour n'importe quel motif. Nous vivons dans un État de droit: on peut être radical, la liberté d'expression est la règle. Tous les salafistes et toutes les personnes nourrissant des sympathies d'extrême droite ou d'extrême gauche ne figurent pas sur cette liste. Ce n'est qu'en cas d'indices qu'une personne représente une menace pour la sécurité nationale que celle-ci y figurera. Il faut en outre préciser que ce n'est pas parce qu'une entité n'est pas reprise dans la banque de données commune que celle-ci ne constitue pas un danger pour la sécurité nationale.

L'avis 73.442/2 du Conseil d'État du 7 juin 2023 a été suivi concernant cet article. L'habilitation au Roi pour déterminer les modalités du droit de création est ainsi supprimée.

Art. 18

Afin d'assurer les missions de sécurité qui sont les leurs, il est primordial que les services de base et les services partenaires qui bénéficient indissociablement d'un droit de lecture et d'un droit d'écriture consultent et alimentent régulièrement la banque de données commune T.E.R. Ce principe, prévu à l'article 44/11/3^{ter}, § 4, de la loi sur la fonction de police, est désormais rappelé à l'alinéa 1^{er} de l'article 18.

de gegevensbanken van het openbaar ministerie pas kan worden aangenomen "na eensluidend advies van het College van procureurs-generaal".

Er wordt verwezen naar de bespreking bij artikel 14 met betrekking tot het advies van Comité I van 13 juli 2023 betreffende de "need to know" (§ 7).

Afdeling 6

*Creatie van een entiteit en voeding
van de gemeenschappelijke gegevensbank T.E.R.*

Art. 17

Artikel 17 herneemt het beginsel van artikel 9 van het koninklijk besluit "TF" en het koninklijk besluit "HP" op grond waarvan enkel een basisdienst een entiteit kan creëren en dus registreren in de gemeenschappelijke gegevensbank (creatierecht).

Er moet op gewezen worden dat de opnamen in de gemeenschappelijke gegevensbank T.E.R. objectief moeten gebeuren. Er zijn duidelijke, wettelijk verankerde criteria die moeten gevolgd worden voor een opname in de gemeenschappelijke gegevensbank T.E.R. Niet iedere entiteit wordt om eender welke reden opgenomen. We leven in een rechtsstaat: radicaal zijn mag, de vrijheid van meningsuiting is de regel. Niet elke salafist, niet elke persoon met rechtsextremistische of linksextremistische sympathieën wordt opgenomen op die lijst. Het is pas als er aanwijzingen zijn dat een persoon een gevaar vormt voor de nationale veiligheid, dat men hierop terechtkomt. Ook moet duidelijk worden gemaakt dat het feit dat een entiteit niet in de gemeenschappelijke gegevensbank is opgenomen, niet betekent dat zij geen gevaar vormt voor de nationale veiligheid.

Advies nr. 73.442/2 van 7 juni 2023 van de Raad van State is voor dit artikel gevolgd. De machtiging aan de Koning om de nadere regels voor het creatierecht te bepalen, wordt dus geschrapt.

Art. 18

Om hun veiligheidsopdrachten te waarborgen, is het essentieel dat de basisdiensten en de partnerdiensten die een onlosmakelijk verbonden leesrecht en schrijfrecht hebben, de gemeenschappelijke gegevensbank T.E.R. geregeld raadplegen en voeden. Dit beginsel, bepaald in artikel 44/11/3^{ter}, § 4 van de wet op het politieambt, wordt thans opnieuw vermeld in het eerste lid van artikel 18.

Comme c'est le cas actuellement, seules les données à caractère personnel et les informations pertinentes, issues des propres banques de données ou fichiers des services de base et des services partenaires, sont reprises dans la banque de données commune T.E.R.

Dans son avis du 13 juillet 2023, le Comité R s'interroge sur l'obligation de contribuer à la banque de données commune T.E.R. pour les services de renseignement et de sécurité (§ 38). En tant que service de base, les services de renseignements doivent alimenter la banque de données commune. Cette alimentation se fait dans le respect des règles générales de classification. Ainsi les services de renseignement vont vérifier, sur base de la législation relative à la classification, si des informations pertinentes peuvent être déclassifiées pour être reprises dans la banque de données commune T.E.R. Par ailleurs, les informations classifiées peuvent être échangées en TFL entre personnes titulaires d'une habilitation de sécurité d'un niveau correspondant.

L'article précise également que les services de base ou les services partenaires qui alimentent la banque de données commune T.E.R. par le biais de leur droit d'écriture ne peuvent se voir opposer l'article 458 du Code pénal relatif à la violation du secret professionnel dans ce contexte. Dans leur avis, l'Autorité de protection des données (Avis n° 97/2023 du 16 juin 2023, §§ 49-52) et le Comité R (Avis du 13 juillet 2023, § 23) se demandent si cette disposition ne crée pas une nouvelle exception à l'article 458 du Code pénal, auquel cas, cette exception devrait y être introduite. Sur ce point, il faut préciser que l'article 458 du Code pénal punit d'un emprisonnement d'un an à trois ans et/ou d'une amende de cent euros à mille euros, les médecins, chirurgiens, officiers de santé, pharmaciens, sage-femmes et toutes autres personnes dépositaires, par état ou par profession, des secrets qu'on leur confie, qui les auront révélés. Cet article prévoit des exceptions à l'application de l'article 458 lorsque la loi oblige l'intéressé à faire connaître ce secret ou lorsqu'il doit témoigner en justice ou devant une commission d'enquête parlementaire. La présente disposition entre clairement dans la première exception dans la mesure où les services de base et les services partenaires qui sont détenteurs du secret professionnel alimentent la banque de données commune, y compris avec des données couvertes par leur secret professionnel, sans pouvoir être accusés d'une violation du secret professionnel. Il ne s'agit dès lors pas d'une nouvelle exception à l'article 458 du Code pénal mais uniquement d'une application d'une exception existante (l'obligation légale).

Zoals thans het geval is, zijn enkel de relevante persoonsgegevens en informatie die afkomstig zijn van de eigen gegevensbanken of bestanden van de basisdiensten en partnerdiensten opgenomen in de gemeenschappelijke gegevensbank T.E.R.

In het advies van 13 juli 2023 heeft Comité I vragen bij de verplichting voor de inlichtingen- en veiligheidsdiensten om bij te dragen tot de gemeenschappelijke gegevensbank T.E.R. (§ 38). Als basisdienst moeten de inlichtingendiensten de gemeenschappelijke gegevensbank aanvullen. Dat gebeurt met inachtneming van de algemene classificatieregels. Aldus zullen de inlichtingendiensten op basis van de classificatiewetgeving nagaan of er relevante informatie kan worden gedeclineerd om in de gemeenschappelijke gegevensbank T.E.R. op te nemen. Voorts kan geclassificeerde informatie in de LTF worden uitgewisseld tussen personen met een veiligheidsmachtiging van een overeenstemmend niveau.

Het artikel bepaalt ook dat artikel 458 van het Strafwetboek betreffende de schending van het beroepsgeheim in deze context niet kan worden opgeworpen tegen de basisdiensten of partnerdiensten die de gemeenschappelijke gegevensbank T.E.R. voeden via hun schrijfrecht. In hun adviezen vragen de Gegevensbeschermingsautoriteit (advies nr. 97/2023 van 16 juni 2023, §§ 49-52) en Comité I (advies van 13 juli 2023, § 23) zich af of die bepaling geen nieuwe uitzondering op artikel 458 van het Strafwetboek schept, in welk geval die uitzondering erin zou moeten worden opgenomen. Daarover moet worden verduidelijkt dat artikel 458 van het Strafwetboek geneesheren, heelkundigen, officieren van gezondheid, apothekers, vroedvrouwen en alle andere personen die uit hoofde van hun staat of beroep kennis dragen van geheimen die hun zijn toevertrouwd, en deze bekendmaken, worden gestraft met gevangenisstraf van een jaar tot drie jaar en/of een geldboete van honderd euro tot duizend euro. Dit artikel voorziet in uitzonderingen op de toepassing van artikel 458 wanneer de wet de belanghebbende verplicht om dat geheim bekend te maken of om in rechte of voor een parlementaire onderzoekscommissie getuigenis af te leggen. Deze bepaling kadert duidelijk binnen de eerste uitzondering, aangezien de basisdiensten en partnerdiensten die houder zijn van een beroepsgeheim, de gemeenschappelijke gegevensbank aanvullen, onder andere met gegevens waarop hun beroepsgeheim betrekking heeft, zonder dat zij ervan kunnen worden beschuldigd het beroepsgeheim te hebben geschonden. Bijgevolg gaat het niet om een nieuwe uitzondering op artikel 458 van het Strafwetboek, maar louter om een toepassing van een reeds bestaande uitzondering (wettelijke verplichting).

Plus particulièrement, concernant l'avis du Comité R sur le secret professionnel relatif aux professionnels de la santé, il faut rappeler que la banque de données commune T.E.R. ne permet pas à ce que des professionnels de la santé, dans le cadre de leur mission thérapeutique, de communiquer des données relatives à la santé. Seuls les services de base et les services partenaires alimentent la banque de données commune. Les données relatives à la santé enregistrées dans la banque de données commune le sont sur base de missions légales qui autorisent cet usage par des professionnels dans le cadre de l'évaluation d'un individu (et en dehors d'un contexte médical). C'est le cas par exemple dans le contexte des établissements pénitentiaires explicité plus haut (cf. exposé des motifs de l'article 6). Le but n'est dès lors pas d'avoir une ouverture plus large du secret professionnel du monde médical vers les services de base et les services partenaires. Le secret médical du médecin reste dès lors protégé. Par ailleurs, comme le rappelle l'Autorité de protection des données dans son avis n° 97/2023 du 16 juin 2023, le traitement des données relatives à la santé ne se confond pas avec la communication d'un dossier médical à laquelle les articles 9 et 10 de la loi du 22 août 2002 relative aux droits du patient continuent à s'appliquer (§ 100).

Enfin, l'auteur du projet confirme, en réponse à un questionnaire du Comité R (§ 23 de son avis du 13 juillet 2023), que, l'objectif n'est pas de modifier implicitement l'article 2, § 2, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité en ce qui concerne le traitement de données protégées par le secret professionnel d'un médecin.

Concernant le Ministère public, il peut être renvoyé à l'article 16, dernière alinéa et il faut rappeler qu'actuellement, conformément à la circulaire COL 18/2020 du Collèges des procureurs généraux, le magistrat de référence "Terrorisme" du ministère public ou du parquet général compétent (titulaire du dossier) informe l'OCAM, à sa demande, des mesures judiciaires suivantes (aussi dans des dossiers non terroristes) relatives aux entités: la détention préventive, la détention préventive sous surveillance électronique, la remise en liberté sous conditions, l'existence d'un mandat d'arrêt international, l'existence d'un mandat d'arrêt européen, la fixation d'une affaire pénale devant le tribunal correctionnel, la cour d'appel et la cour d'assises, la condamnation/ l'acquittement pour une infraction terroriste (articles 137 à 141 Code pénal). Ils peuvent communiquer ces mesures judiciaires soit par mail, soit en les insérant dans les banques de données "TF" et "PH" actuelles si c'est faisable sur le plan technique et avec l'accord du responsable opérationnel (l'OCAM) et le gestionnaire (la police fédérale). La

Meer in het bijzonder wat het advies van Comité I over het beroepsgeheim bij gezondheidswerkers betreft, moet erop worden gewezen dat zij via de gemeenschappelijke gegevensbank T.E.R. niet de mogelijkheid hebben om gezondheidsgelateerde gegevens te delen in het kader van hun gezondheidsgelateerde opdracht. Enkel de basisdiensten en partnerdiensten vullen de gemeenschappelijke gegevensbank aan. De in de gemeenschappelijke gegevensbank opgenomen gezondheidsgelateerde gegevens zijn dat op basis van wettelijke opdrachten op basis waarvan professionals daarvan gebruik mogen maken in het kader van de evaluatie van een individu (en buiten een medische context). Dat is bijvoorbeeld het geval in de hierboven vermelde context van de penitentiaire inrichtingen (zie memorie van toelichting bij artikel 6). Het is dus niet het doel het beroepsgeheim te verruimen vanuit de medische wereld naar de basisdiensten en partnerdiensten. Het beroepsgeheim van de arts blijft dus beschermd. Voorts is het, zoals de Gegevensbeschermingsautoriteit opmerkt in advies nr. 97/2023 van 16 juni 2023, zo dat de verwerking van gegevens met betrekking tot de gezondheid niet hetzelfde is als de mededeling van een medisch dossier, waarop de artikelen 9 en 10 van de wet van 22 augustus 2002 betreffende de rechten van de patiënt van toepassing blijven (§ 100).

Tot slot bevestigt de auteur van het ontwerp in antwoord op een vraag van Comité I (§ 23 van het advies van 13 juli 2023) dat het niet de bedoeling is om artikel 2, § 2, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten impliciet te wijzigen voor wat betreft de verwerking van gegevens die worden beschermd door het beroepsgeheim van een arts.

Wat het Openbaar Ministerie betreft, kan worden verwezen naar artikel 16, laatste lid en wordt eraan herinnerd dat momenteel, overeenkomstig de omzendbrief COL 18/2020 van het College van procureurs-generaal, de referentiemagistraat "Terrorisme" van het bevoegde (titularis van het dossier) openbaar ministerie of parket-generaal het OCAD informeert, op diens vraag, over de volgende gerechtelijke maatregelen (ook in niet-terroristische dossiers) met betrekking tot de entiteiten: de voorlopige hechtenis, de voorlopige hechtenis onder elektronisch toezicht, de vrijlating onder voorwaarden, het bestaan van een internationaal aanhoudingsbevel, het bestaan van een Europees aanhoudingsbevel, de vaststelling van een strafzaak voor de correctionele rechtbank, het hof van beroep of het hof van assisen, de veroordeling/vrijspraak voor een terroristisch misdrijf (artikel 137 -141 Strafwetboek). Zij kunnen deze gerechtelijke maatregelen mededelen, hetzij via e-mail, hetzij door deze in te brengen in de huidige gegevensbanken "TF" en "HP" indien dit technisch mogelijk is en met

demande initiale doit explicitement émaner de l'OCAM, mais les modifications de ces mesures judiciaires sont ensuite communiquées d'initiative à l'OCAM. Lorsque la personne concernée fait l'objet d'une enquête fédérale cette notification à l'OCAM est faite, à sa demande, par le parquet fédéral en ce qui concerne les informations relatives aux dossiers fédéraux.

Pour rappel, le Collège des procureurs généraux prendra une circulaire nationale avec des directives contraignantes à ce sujet. On peut raisonnablement s'attendre à ce que dorénavant le ministère public communique d'initiative les informations judiciaires suivantes: la détention préventive; la détention préventive sous surveillance électronique; la remise en liberté sous conditions; l'existence d'un mandat d'arrêt international; l'existence d'un mandat d'arrêt européen; la décision des juridictions d'instruction statuant sur le fond (l'internement et la suspension du prononcé); la fixation d'une affaire pénale devant le tribunal correctionnel, la cour d'appel et la cour d'assises et la condamnation/l'acquittement.

L'article 18, alinéa 1^{er}, contient également le principe de validation interne des données à caractère personnel et informations que les services de base et les services partenaires introduisent dans la banque de données commune T.E.R. (Art. 44/11/3^{ter}, § 4, de la loi sur la fonction de police).

Il est important de rappeler qu'il existe deux niveaux de validation. Le premier au moment de l'alimentation de la banque de données commune selon les procédures internes de validation, propres à chaque service pour s'assurer du respect des modalités de traitement définies. C'est celui-ci dont il est question dans le présent article. Les procédures internes de validation permettent, entre autres, aux services qui doivent alimenter la banque de données commune T.E.R. de démontrer le respect des obligations qui s'imposent à eux en matière de qualité des données à caractère personnel et des informations comme décrit à l'article 30, § 1^{er}, 1^o et § 2. Le second niveau de validation existe au moment du contrôle des données et informations dans la banque de données commun par le responsable opérationnel (cf. *infra*).

Il convient également de préciser que pour accéder à la banque de données commune T.E.R., les services de base et les services partenaires désignent les membres de leur organisation qui accèdent aux données à caractère personnel et informations de la banque de données commune T.E.R. et que ces membres sont titulaires d'une

akkoord van de operationeel verantwoordelijke (het OCAD) en de beheerder (de Federale Politie). De initiële vraag dient expliciet uit te gaan van het OCAD, maar de wijzigingen van deze gerechtelijke maatregelen worden nadien op eigen initiatief meegedeeld aan het OCAD. Wanneer de betrokken persoon het voorwerp uitmaakt van een federaal onderzoek gebeurt deze kennisgeving aan het OCAD, op diens vraag, door het federaal parket wat de informatie in federale dossiers betreft.

Ter herinnering: het College van procureurs-generaal zal een nationale omzendbrief met bindende richtlijnen hierover uitvaardigen. Er kan redelijkerwijze worden verwacht dat het Openbaar Ministerie voortaan de volgende gerechtelijke gegevens op eigen initiatief zou mededelen: de voorlopige hechtenis; de voorlopige hechtenis onder elektronisch toezicht; de vrijlating onder voorwaarden; het bestaan van een internationaal aanhoudingsbevel; het bestaan van een Europees aanhoudingsbevel; de beslissing van de onderzoeksgerechten zetelend ten gronde (de internering en de opschorting van de uitspraak); de vaststelling van een strafzaak voor de correctionele rechtbank, het hof van beroep of het hof van assisen en de veroordeling/vrijpraak.

Artikel 18, eerste lid, bevat ook het beginsel inzake interne validering van de persoonsgegevens en de informatie die de basisdiensten en de partnerdiensten in de gemeenschappelijke gegevensbank T.E.R. invoeren (Art. 44/11/3^{ter}, § 4, van de wet op het politieambt).

Het is belangrijk erop te wijzen dat er twee validatieniveaus zijn. Het eerste op het moment van de voeding van de gemeenschappelijke gegevensbank volgens de interne validatieprocedures die eigen zijn aan elke dienst om te waarborgen dat de omschreven nadere regels voor de verwerking worden nageleefd. Dat is het niveau waar het in dit artikel om gaat. De interne validatieprocedures maken het de diensten die de gemeenschappelijke gegevensbank T.E.R. moeten voeden onder andere mogelijk om aan te tonen dat de verplichtingen die hun worden opgelegd inzake de kwaliteit van de persoonsgegevens en de informatie, zoals omschreven in artikel 30, § 1, 1^o, en § 2, worden nageleefd. Het tweede validatieniveau situeert zich op het moment dat de gegevens en informatie in de gemeenschappelijke gegevensbank worden gecontroleerd door de operationeel verantwoordelijke (cf. *infra*).

Er moet tevens worden verduidelijkt dat, om toegang te krijgen tot de gemeenschappelijke gegevensbank T.E.R., de basisdiensten en de partnerdiensten de leden van hun organisatie aanwijzen die toegang hebben tot de persoonsgegevens en informatie van de gemeenschappelijke gegevensbank T.E.R. en dat die leden houder zijn

habilitation de sécurité du degré “secret “. Ce principe est actuellement prévu à l'article 7, § 2, de l'arrêté royal “TF” et de l'arrêté royal “PH”.

L'alinéa 4, de l'article 18, est nouveau par rapport au cadre existant et prévoit que “Les services de police saisissent les données à caractère personnel et les informations visées à l'alinéa 1^{er}, conformément aux spécifications supplémentaires énoncées dans une directive du Collège des procureurs généraux visant à sauvegarder le secret de l'instruction tel que prévu aux articles 28quinquies et 57 du Code d'instruction criminelle et l'exercice de l'action publique.”

En effet, une précision doit être faite dans le cas de la police, en particulier pour la police lorsqu'elle traite des données à caractère judiciaire (la police judiciaire fédérale et les services de recherche de la police locale). Ainsi la circulaire COL 18/2020 du Collège des procureurs généraux prévoit à l'heure actuelle déjà que les données à caractère personnel et informations suivantes ne seront pas transmises à la banque de données commune T.E.R. et n'y seront donc pas reprises:

- les données à caractère personnel et informations classifiées;

- les données à caractère personnel et informations provenant des mesures d'enquête (p.ex. l'écoute téléphonique, le contrôle visuel discret, etc.) ou des méthodes particulières de recherche (le recours aux informateurs, l'observation, l'infiltration et l'infiltration civile) prises dans le cadre d'une enquête pénale à l'insu de la personne intéressée;

- les données à caractère personnel et informations qui ont été placées sous “embargo judiciaire BDC” (visé par l'article 19).

Le raisonnement du C.O.C. concernant cet article dans son avis du 20 juin 2023, est bien correct: les informations policières provenant de “RIR, codes 01 ou 00” pourront être reprises dans la banque de données commune T.E.R.

Au sujet de cet article encore, le Conseil d'État, dans son avis 73.442/2 du 7 juin 2023, indique ce qui suit:

“Compte tenu de l'obligation pesant sur les services partenaires d'introduire dans la banque de données les données à caractère personnel et les informations dont ils disposent, il s'indiquera de préciser les modalités qui permettront à ces services d'être informés de la création d'une “entité” dans la banque de données. À défaut, les services concernés seraient confrontés à l'obligation de

van een veiligheidsmachtiging van het niveau “geheim”. In dit beginsel is thans voorzien in artikel 7, § 2, van het koninklijk besluit “TF” en het koninklijk besluit “HP”.

Lid 4 van artikel 18 is nieuw ten opzichte van het bestaande kader en bepaalt dat “De politiediensten voeren de persoonsgegevens en informatie bedoeld in het eerste lid in, overeenkomstig de nadere specificaties opgenomen in een richtlijn van het College van procureurs-generaal strekkende tot de vrijwaring van het geheim van het onderzoek zoals vastgelegd in de artikelen 28quinquies en 57 van het Wetboek van Strafvordering en van de uitoefening van de strafvordering.”

Wat de politie betreft, met name voor de politie wanneer deze gegevens van gerechtelijke aard verwerkt (Federale gerechtelijke politie en lokale recherche-diensten) moet inderdaad een verduidelijking worden bepaald. Zo bepaalt de omzendbrief COL 18/2020 van het College van procureurs-generaal op dit ogenblik al dat de volgende persoonsgegevens en informatie niet aan de gemeenschappelijke gegevensbank T.E.R. kunnen worden toegezonden en er bijgevolg niet in worden opgenomen:

- geclassificeerde persoonsgegevens en informatie;

- persoonsgegevens en informatie afkomstig van onderzoeksmaatregelen (bijvoorbeeld telefoontap, in-kijkoperatie, enz.) en bijzondere opsporingsmethoden (informantenwerking, observatie, infiltratie en burgerinfiltratie) die lopende zijn in een strafonderzoek zonder medeweten van de betrokken persoon;

- persoonsgegevens en informatie die onder “gerechtelijk embargo GGB” staan (bedoeld in artikel 19).

De redenering van het COC met betrekking tot dit artikel in het advies van 20 juni 2013 is correct: politionele informatie afkomstig van “RIR, codes 01 of 00” zullen in de gemeenschappelijke gegevensbank T.E.R. kunnen worden opgenomen.

De Raad van State geeft in advies nr. 73.442/2 van 7 juni 2023 over dit artikel nog het volgende aan:

“Rekening houdend met het feit dat de partnerdiensten verplicht zijn om de persoonsgegevens en de informatie waarover ze beschikken, in de gegevensbank in te voeren, dienen de nadere regels te worden gespecificeerd op basis waarvan die diensten worden geïnformeerd zodra een “entiteit” in de gegevensbank wordt gecreëerd. Zo niet zouden de betrokken diensten zich verplicht zien op

se tenir informés à leur initiative de l'éventualité de la création d'une "entité" à propos de laquelle ils disposeraient de données ou d'informations, ce qui, sur le plan pratique, ne saurait se concevoir que difficilement."

Les obligations qui incombent aux services partenaires en application des droits de lecture et d'écriture sont les mêmes que celles qui existent actuellement. Le système actuel fonctionne correctement et n'a pas posé de difficultés jusqu'à ce jour. Aucun besoin n'a été exprimé au sujet de la communication de la création d'une "entité" dans la banque de données. Dans les faits et le cas échéant, un service sera informé de la création d'une entité car soit elle aura fait l'objet d'une discussion en TLF, soit un service sera informé en vérifiant la banque de données commune en raison du dossier qu'il traite.

Art. 19

L'article 19 reprend le principe selon lequel le droit de création et le droit d'écriture dans la banque de données commune T.E.R. peuvent être différés lorsque et aussi longtemps que le magistrat compétent, avec l'accord du procureur fédéral, estime que cette création et cette alimentation peuvent compromettre l'exercice de l'action publique ou la sécurité d'une personne mais également la relation avec un service répressif d'un État étranger.

L'article 19 prévoit désormais que le droit de création peut également être différé par un magistrat. Il s'agit d'une nouvelle possibilité prévue par l'article 19 car l'article 44/11/3^{ter}, § 5, ne prévoyait cette possibilité que pour l'alimentation de la banque de données commune et donc pour le nouveau droit d'écriture des services de base et des services partenaires.

Le fait qu'une entité soit enregistrée dans la banque de données commune T.E.R. peut dans certaines situations, effectivement, poser question. En effet, un tel enregistrement fait apparaître clairement à l'entité concernée qu'elle fait l'objet de poursuites, ce qui peut compromettre l'exercice de l'action publique ou la sécurité d'une personne.

En ce qui concerne le fait de compromettre la relation avec un service répressif d'un État étranger, il faut préciser qu'en application de l'article 8, paragraphes 3 et 4, de la décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne, "3. les informations et les renseignements communiqués

eigen initiatief op de hoogte te blijven van de eventuele creatie van een "entiteit" waarover ze gegevens en informatie zouden hebben, wat praktisch gezien maar moeilijk denkbaar zou zijn."

De verplichtingen voor de partnerdiensten overeenkomstig de lees- en schrijfrechten zijn dezelfde als die die momenteel bestaan. Het huidige systeem werkt goed en heeft tot nog toe geen problemen veroorzaakt. Er is geen behoefte geuit over het meedelen van de creatie van een "entiteit" in de gegevensbank. In de praktijk en in voorkomend geval wordt een dienst in kennis gesteld van de creatie van een entiteit, ofwel omdat daarover is gesproken in een TLF, ofwel omdat een dienst in kennis wordt gesteld door de gemeenschappelijke gegevensbank te controleren in het kader van het dossier dat hij behandelt.

Art. 19

In artikel 19 is het beginsel opgenomen dat het creatierecht en het schrijfrecht in de gemeenschappelijke gegevensbank T.E.R. kunnen worden uitgesteld wanneer en zolang de bevoegde magistraat, met toestemming van de federale procureur, meent dat deze creatie en deze voeding de uitoefening van de strafvordering, de veiligheid van een persoon of de relatie met een rechtshandhavingsautoriteit van een buitenlandse Staat in het gedrang kunnen brengen.

In artikel 19 wordt voortaan bepaald dat het creatierecht eveneens kan worden uitgesteld door een magistraat. Het betreft een nieuwe mogelijkheid waarin in artikel 19 wordt voorzien, want in artikel 44/11/3^{ter}, § 5, werd alleen in deze mogelijkheid voorzien voor de voeding van de gemeenschappelijke gegevensbank, en dus voor het nieuwe schrijfrecht van de basisdiensten en de partnerdiensten.

Het feit dat een entiteit in de gemeenschappelijke gegevensbank T.E.R. is opgenomen, kan in bepaalde situaties wel degelijk vragen oproepen. Een dergelijke registratie wijst er bij de betrokken entiteit namelijk duidelijk op dat ze het voorwerp uitmaakt van opvolging, wat de uitoefening van de strafvordering of de veiligheid van een persoon in gevaar kan brengen.

Wat betreft het in het gedrang brengen van de relatie met een rechtshandhavingsautoriteit van een buitenlandse Staat moet het volgende worden verduidelijkt: artikel 8, leden 3 en 4, van het kaderbesluit 2006/960/JBZ van de Raad van 18 december 2006 betreffende de vereenvoudiging van de uitwisseling van informatie en inlichtingen tussen de rechtshandhavingsautoriteiten van de lidstaten van de Europese Unie, bepaalt: "3. De

au titre de la présente décision-cadre ne peuvent être utilisés par les services répressifs compétents de l'État membre auxquels ils ont été transmis qu'aux fins pour lesquelles ils ont été communiqués conformément à la présente décision-cadre ou pour prévenir un danger immédiat et sérieux pour la sécurité publique; leur traitement à d'autres fins n'est autorisé qu'avec l'accord préalable de l'État membre émetteur et sous réserve du droit national de l'État membre destinataire. L'accord peut être donné pour autant que le droit national de l'État membre émetteur le permette.

4. Lorsqu'ils transmettent des informations et des renseignements au titre de la présente décision-cadre, les services répressifs compétents peuvent, en application de leur droit national, imposer aux services répressifs destinataires des conditions concernant l'usage qu'ils feront de ces informations et renseignements. Des conditions peuvent aussi être imposées en ce qui concerne la diffusion des résultats de l'enquête pénale ou de l'opération de renseignement en matière pénale qui a donné lieu à l'échange d'informations et de renseignements. Les services répressifs destinataires des informations et des renseignements sont liés par de telles conditions, sauf dans le cas particulier où le droit national oblige à déroger aux restrictions d'utilisation au profit des autorités judiciaires, des institutions législatives ou de toute autre instance indépendante créée par la loi et chargée du contrôle des services répressifs compétents. Dans ce cas, les informations et les renseignements ne peuvent être utilisés qu'après consultation préalable de l'État membre émetteur dont les intérêts et points de vue doivent être pris en compte autant que possible. L'État membre destinataire peut, dans des cas particuliers, être invité par l'État membre émetteur à donner des informations sur l'utilisation et le traitement ultérieur des informations et renseignements transmis."

Au regard de ce qui précède, l'introduction d'une information fournie par un service répressif d'un État étranger dans la banque de données commune T.E.R. requiert donc l'accord préalable de l'État étranger émetteur.

Dans le cas de réserves émises par l'État étranger émetteur, il appartient au magistrat compétent de décider de différer ce droit de création et ce droit d'écriture en prenant en compte les conditions imposées par l'État étranger ou l'instrument juridique international sur base duquel l'État étranger a transmis les informations concernées. Comme prévu dans l'article de loi ("le cas échéant le procureur fédéral peut déterminer les modalités

information et inlichtingen die krachtens dit kaderbesluit worden verstrekt, mogen door de bevoegde rechtshandhavingsautoriteiten van de ontvangende lidstaat alleen worden gebruikt ten behoeve van de doeleinden waarvoor zij overeenkomstig dit kaderbesluit zijn verstrekt of ter voorkoming van een onmiddellijke en ernstige bedreiging van de openbare veiligheid; verwerking voor andere doeleinden is alleen toegestaan na voorafgaande toestemming van de verstreckende lidstaat en wordt beheerst door het nationale recht van de ontvangende lidstaat. De toestemming kan worden verleend voor zover het nationale recht van de verstreckende lidstaat daarin voorziet.

4. Bij het verstrekken van informatie en inlichtingen overeenkomstig dit kaderbesluit kan de verstreckende bevoegde rechtshandhavingsautoriteit op grond van het nationale recht voorwaarden opleggen betreffende het gebruik van de informatie en inlichtingen door de ontvangende bevoegde rechtshandhavingsautoriteit. Tevens kunnen voorwaarden worden opgelegd betreffende de rapportage over het resultaat van het strafrechtelijk onderzoek of de criminele-inlichtingenoperatie in het kader waarvan de uitwisseling van informatie en inlichtingen heeft plaatsgevonden. Deze voorwaarden zijn bindend voor de ontvangende bevoegde rechtshandhavingsautoriteit, behalve in het specifieke geval waarin het nationale recht bepaalt dat de beperkingen van het gebruik worden opgeheven voor rechterlijke instanties, wetgevende organen of andere uit hoofde van de wet opgerichte onafhankelijke lichamen waaraan een bevoegdheid tot toezicht op de bevoegde rechtshandhavingsautoriteiten is verleend. In dat geval mogen de informatie en inlichtingen slechts worden gebruikt na voorafgaande raadpleging van de verstreckende lidstaat, waarvan de belangen en standpunten zoveel mogelijk in aanmerking moeten worden genomen. In specifieke gevallen kan de verstreckende lidstaat de ontvangende lidstaat verzoeken informatie te verstrekken over het gebruik en de verdere verwerking van de verstrekte informatie en inlichtingen."

Gelet op het voorgaande vereist de invoer in de gemeenschappelijke gegevensbank T.E.R. van informatie die door een rechtshandhavingsautoriteit van een buitenlandse Staat werd verstrekt, bijgevolg de voorafgaande toestemming van de verstreckende buitenlandse Staat.

Wanneer de verstreckende buitenlandse Staat voorbehouden maakt, behoort het de bevoegde magistraat toe te beslissen dit creatierecht en dit schrijfrecht uit te stellen, met inachtneming van de voorwaarden die de buitenlandse Staat oplegt of het internationaal recht-instrument op grond waarvan de buitenlandse staat de betrokken informatie heeft verstrekt. Zoals bepaald in het artikel van de wet ("In voorkomend geval kan de

de cette dérogation”), le procureur fédéral peut aussi décider de modalités particulières d’enregistrement de données dans la banque de données commune T.E.R.

L’article 19 prévoit également que le droit de création et le droit d’écriture peuvent être différés lorsque et aussi longtemps que le dirigeant d’un service de renseignement et de sécurité estime que cette création et cette alimentation peuvent compromettre la sécurité d’une personne, l’exercice d’une enquête mais également la relation avec un service de renseignement et de sécurité d’un État étranger. Cette dernière possibilité vise par exemple la situation dans laquelle un service de renseignements et de sécurité étranger a explicitement demandé de ne pas transmettre une information déterminée à d’autres services.

Section 7

Communication

des données à caractère personnel et des informations

Cette section contient l’ensemble des dispositions de la loi sur la fonction de police ou des arrêtés royaux “TF” et “PH” relatives à la communication des données à caractère personnel et des informations.

L’objectif est de centraliser toutes les dispositions relatives à la communication dans une seule section afin d’en simplifier la lecture.

Dans un souci de cohérence, les auteurs de la présente loi ont décidé d’aborder dans la cadre de cette section successivement la communication de la fiche de renseignement, la communication de la création d’une entité au chef de corps, la communication à une autorité ou institution tierce, la communication de la carte d’information, de listes. Enfin, sont également reprises les communications internationales. La communication de l’évaluation de la menace est également traitée dans cette section.

Art. 20

L’article 20 reprend le principe appliqué à la fiche de renseignements visé à l’article 10 de l’arrêté royal “TF” et de l’arrêté royal “PH” selon lequel celle-ci n’est accessible que pour les services qui l’alimentent et la consultent sur base du droit d’écriture et du droit de lecture créés par la nouvelle loi. À noter qu’en application du nouvel article 15, § 1, les autorités de contrôle disposent uniquement d’un droit de lecture dans la banque de données commune T.E.R. À ce titre, la fiche de renseignements ne leur serait plus communiquée.

federale procureur de nadere regels voor deze afwijking bepalen.”), kan de federale procureur eveneens beslissen over bijzondere nadere regels inzake de registratie van gegevens in de gemeenschappelijke gegevensbank T.E.R.

In artikel 19 wordt eveneens bepaald dat het creatierecht en het schrijfrecht kunnen worden uitgesteld wanneer en zolang de leidinggevende van een inlichtingen- en veiligheidsdienst meent dat deze creatie en deze voeding de veiligheid van een persoon, de uitoefening van een onderzoek of de relatie met een inlichtingen- en veiligheidsdienst van een buitenlandse Staat in het gedrang kunnen brengen. Die laatste mogelijkheid beoogt bijvoorbeeld de situatie waarin een buitenlandse inlichtingen- en veiligheidsdienst uitdrukkelijk heeft gevraagd bepaalde informatie niet aan andere diensten toe te zenden.

Afdeling 7

Mededeling

van de persoonsgegevens en informatie

Deze afdeling bevat alle bepalingen van de wet op het politieambt of de koninklijke besluiten “TF” en “HP” met betrekking tot de mededeling van de persoonsgegevens en informatie.

Het is de bedoeling om alle bepalingen met betrekking tot de mededeling in een enkele afdeling te centraliseren om de lezing ervan te vergemakkelijken.

Met het oog op coherentie hebben de auteurs van deze wet beslist om in het kader van deze afdeling achtereenvolgens de mededeling van de inlichtingenfiche, de mededeling van de creatie van een entiteit aan de korpschef, de mededeling aan een derde overheid of een derde instelling, de mededeling van de informatiekaart, van lijsten te behandelen. Ten slotte is ook de internationale mededeling erin opgenomen. Ook de mededeling van de dreigingsevaluatie wordt in deze afdeling behandeld.

Art. 20

Artikel 20 herneemt het principe dat van toepassing is op inlichtingenfiches en vevat zit in artikel 10 van het koninklijk besluit “TF” en het koninklijk besluit “HP”. Volgens dat principe, is de inlichtingenfiche enkel toegankelijk voor de diensten die ze voeden en raadplegen op grond van het schrijfrecht en het leesrecht die bij de nieuwe wet zijn ingevoerd. Er dient te worden opgemerkt dat de toezichthoudende overheden met toepassing van het nieuwe artikel 15, § 1, enkel over een leesrecht in de gemeenschappelijke gegevensbank

Or, pour l'exercice de leurs missions de contrôle visées à l'article 161 de loi relative à la protection des données, il est nécessaire qu'elles puissent disposer d'une vue sur l'ensemble des données traitées dans la banque de données commune T.E.R. Une exception est dès lors introduite pour les autorités de contrôles leur donnant accès à la fiche de renseignements.

Pour ne pas mettre en péril les éventuelles enquêtes dont fait l'objet la personne concernée, certaines informations plus sensibles concernant ces enquêtes ne sont pas reprises sur la fiche de renseignements.

Il en va de même pour les informations relatives aux méthodes de recueil de données mises en œuvre par les services de renseignement et de sécurité qui n'apparaissent pas dans la fiche de renseignements.

Ces données et informations feront en outre *a priori* l'objet d'un embargo tel que prévu à l'article 44/11/3^{ter}, § 5, de la loi sur la fonction de police puisque qu'elles n'alimenteront pas, dans les conditions prévues, la banque de données commune T.E.R.

Art. 21

L'article 21 reprend le principe de l'article 44/11/3^{ter}, § 4, al. 2, de la loi sur la fonction de police. Il concerne la communication au président de la Task force locale visée à l'article 31 et au chef de corps de chaque zone de police concernée de l'enregistrement d'une nouvelle entité dans la banque de données commune. Le principe a été reformulé afin de préciser qu'il s'agit de la création d'une nouvelle entité qui est communiquée au chef de corps mais aussi au président de la Task force locale.

Dans son avis du 20 juin 2023, le C.O.C. se demande si cette disposition s'applique également aux entités en statut de "pré-enquête". La réponse est affirmative.

Art. 22

L'article 22 est nouveau. Il prévoit que sur base du respect des principes d'adéquation, de pertinence et du caractère non excessif dans le cadre de l'exercice de leurs missions respectives – c'est-à-dire la nécessité de prendre connaissance de données à caractère personnel et informations de la banque de données commune T.E.R. pour l'exercice de missions légales – et dans le cadre des finalités visées à l'article 5, alinéa 2, les services partenaires qui, en application de l'article 16,

T.E.R. beschikken. Zodoende zou de inlichtingenfiche hun niet langer worden meegedeeld. Voor de uitoefening van hun in artikel 161 van de wet gegevensbescherming bedoelde controleopdrachten moeten ze echter kunnen beschikken over een overzicht van alle gegevens die in de gemeenschappelijke gegevensbank T.E.R. worden verwerkt. Daarom wordt voor de toezichthoudende overheden een uitzondering ingevoerd die hun toegang verleent tot de inlichtingenfiche.

Om de eventuele onderzoeken waarvan de betrokkene het voorwerp uitmaakt, niet in gevaar te brengen, wordt bepaalde meer gevoeligere informatie betreffende deze onderzoeken niet hernomen op de inlichtingenfiche.

Hetzelfde geldt voor de informatie met betrekking tot de methoden voor gegevensverzameling die door de inlichtingen- en veiligheidsdiensten gebruikt worden en die niet voorkomen op de inlichtingenfiche.

Die gegevens en informatie zijn voorts *a priori* voorwerp van een embargo zoals voorzien in artikel 44/11/3^{ter}, § 5, van de wet op het politieambt aangezien ze volgens de voorziene regels de gemeenschappelijke gegevensbank T.E.R. niet zullen voeden.

Art. 21

Artikel 21 herneemt het beginsel van artikel 44/11/3^{ter}, § 4, tweede lid, van de wet op het politieambt. Het betreft de mededeling aan de voorzitter van de Lokale Task Force bedoeld in artikel 31 en aan de korpschef van elke betrokken politiezone van de registratie van een nieuwe entiteit in de gemeenschappelijke gegevensbank. Het beginsel is geherformuleerd om te verduidelijken dat het gaat om de creatie van een nieuwe entiteit die aan de korpschef maar ook aan de voorzitter van de Lokale Task Force wordt meegedeeld.

In het advies van 20 juni 2023 vraagt het COC of deze bepaling ook van toepassing is op de entiteiten in "vooronderzoek". Het antwoord is ja.

Art. 22

Artikel 22 is nieuw. Het bepaalt dat, op basis van de inachtneming van de principes van toereikendheid, relevantie en de niet-bovenmatige aard in het kader van de uitoefening van hun respectieve opdrachten – dat wil zeggen de noodzaak om kennis te nemen van persoonsgegevens en informatie van de gemeenschappelijke gegevensbank T.E.R. voor de uitoefening van wettelijke opdrachten – en in het kader van de doeleinden van artikel 5, tweede lid, de partnerdiensten

disposent d'un droit d'interrogation dans la banque de données commune T.E.R. reçoivent dorénavant en cas de confirmation de l'existence d'une entité validée dans la banque de données commune T.E.R. l'évaluation de la menace.

En effet, l'actuelle interrogation directe prévue par la loi sur la fonction de police et les AR "TF" et "PH", porte sur l'existence de données sur une entité. En cas de confirmation de l'existence d'une entité dans la banque de données, l'interrogation directe ne procure aucune donnée au service qui a interrogé la banque de données. Ce service doit alors contacter un service de base de sorte que ce dernier puisse contextualiser l'information disponible en fonction de ses besoins. Il s'est avéré que pour certaines situations, cette contextualisation n'était pas suffisante pour permettre au service qui a procédé à l'interrogation d'exercer ses missions. Pour pallier cette lacune, le nouvel article 22 prévoit que sur base du respect des principes d'adéquation, de pertinence et du caractère non excessif, dans le cadre de l'exercice de leurs missions respectives et dans le cadre des finalités visées à l'article 5, alinéa 2, le service partenaire qui a utilisé son droit d'interrogation (actuelle interrogation directe) se voit communiquer l'évaluation de la menace lorsque le droit d'interrogation a confirmé l'existence d'une entité validée dans la banque de données commune T.E.R.

À noter toutefois, que malgré la réception de l'évaluation de la menace, le destinataire a l'obligation de contacter un service de base de sorte que ce dernier puisse non seulement mieux contextualiser l'information disponible dans l'évaluation de menace en fonction du destinataire mais aussi de faire part lors de la prochaine task force que le dossier de la personne évolue. À noter que chaque service partenaire a ses propres canaux pour contacter un service de base. Toutefois, dans l'hypothèse où un service partenaire n'aurait pas encore établi un tel canal privilégié, il s'adressera par défaut à l'OCAM en sa qualité de service de base et de responsable opérationnel.

Il est renvoyé au commentaire de l'article 14 en ce qui concerne l'avis du Comité R du 13 juillet 2023 relatif au "besoin d'en connaître" (§ 7).

Art. 23

L'article 23, alinéa 1^{er}, reprend le contenu de l'article 44/11/3^{quater} de la loi sur la fonction de police. Il concerne les deux conditions selon lesquelles la carte d'information peut être communiquée à des destinataires autres que ceux visés aux articles précédents.

die overeenkomstig artikel 16 over een vraagrecht in de gemeenschappelijke gegevensbank T.E.R. beschikken, voortaan de dreigingsevaluatie ontvangen in geval van bevestiging van het bestaan van een gevalideerde entiteit in de gemeenschappelijke gegevensbank T.E.R.

De huidige rechtstreekse bevraging waarin in de wet op het politieambt en in de KB's "TF" en "HP" wordt voorzien, heeft betrekking op het bestaan van gegevens over een entiteit. In geval van bevestiging van het bestaan van een entiteit in de gegevensbank worden bij de rechtstreekse bevraging geen gegevens verstrekt aan de dienst die de gegevensbank heeft bevroegd. Die dienst moet dan contact opnemen met een basisdienst die de beschikbare informatie kan contextualiseren, naargelang zijn noden. Voor sommige situaties bleek die contextualisering niet voldoende om de dienst die de bevraging heeft uitgevoerd in staat te stellen zijn opdrachten uit te voeren. Om die tekortkoming te verhelpen, wordt in het nieuwe artikel 22 bepaald dat op basis van de inachtneming van principes van toereikendheid, relevantie en de niet-bovenmatige aard in het kader van de uitoefening van zijn respectieve opdrachten en in het kader van de doeleinden van artikel 5, tweede lid, de partnerdienst die zijn vraagrecht heeft aangewend (huidige rechtstreekse bevraging), de dreigingsevaluatie ontvangt wanneer aan de hand van het vraagrecht het bestaan van een gevalideerde entiteit in de gemeenschappelijke gegevensbank T.E.R. wordt bevestigd.

Er moet evenwel worden opgemerkt dat, ondanks de ontvangst van de dreigingsevaluatie, de bestemming verplicht is contact op te nemen met een basisdienst die niet alleen de beschikbare informatie op de dreigingsevaluatie beter kan contextualiseren naargelang van de bestemming, maar tevens bij de volgende taskforce kan melden dat het dossier van de persoon evolueert. Er zij op gewezen dat elke partnerdienst zijn eigen kanalen heeft om contact op te nemen met een basisdienst. Ingeval een partnerdienst evenwel nog geen dergelijk geprivilegieerd kanaal heeft, richt hij zich standaard tot het OCAD in diens hoedanigheid van basisdienst en operationeel verantwoordelijke.

Er wordt verwezen naar de bespreking bij artikel 14 met betrekking tot het advies van Comité I van 13 juli 2023 betreffende de "need to know" (§ 7).

Art. 23

Artikel 23, eerste lid, herneemt de inhoud van artikel 44/11/3^{quater} van de wet op het politieambt. Het betreft de twee voorwaarden waaronder de informatiekaart kan worden meegedeeld aan andere bestemmingen dan degenen die in de voorgaande artikelen worden

Moyennant le respect des conditions prévues dans cet article et à l'article 24, il peut s'agir ici de personnes individuelles. Dans son avis n° 97/2023 du 16 juin 2023, l'Autorité de protection des données indique que le principe d'une communication basée sur le besoin d'en connaître implique une évaluation en fonction des (catégories de) données et non de l'ensemble d'un support (la carte d'information) (§ 65). À ce sujet, on peut renvoyer à la définition de la carte d'information selon laquelle elle consiste en un extrait de la fiche de renseignements, contenant les données à caractère personnel et informations, adéquates, pertinentes et non excessives au destinataire pour le suivi des entités. Il s'agit donc d'une carte d'information "sur mesure". Il est également renvoyé au commentaire de l'article 14 en ce qui concerne l'avis du Comité R du 13 juillet 2023 relatif au "besoin d'en connaître" (§ 7).

Autre exemple: il se peut qu'un des services qui bénéficie d'un droit de lecture et d'un droit d'écriture dans la banque de données commune T.E.R. estime qu'il est nécessaire de fournir tout ou partie des données à caractère personnel à une ASBL ou à une école afin de prévenir un départ d'un jeune en décrochage social vers la Syrie. Dans ce cas, les services qui sont à la base des informations doivent évaluer préalablement à cette communication si celle-ci est bénéfique à tout le monde ainsi que les conditions relatives à cette communication, sur la base des modalités déterminées à l'article 24.

Afin d'éviter une confusion avec le terme "entité" tel qu'il est défini à l'article 2, 4° et énoncé à plusieurs reprises dans le projet, celui-ci a été remplacé par le terme "instance" dans le cadre de l'article 23.

Il convient de préciser que cette communication vis-à-vis de ces destinataires s'effectue sans préjudice des procédures existantes trouvant leur source dans un texte légal tel qu'un arrêté ministériel, un arrêté royal, une loi ou encore une convention internationale. Ainsi, elle ne peut porter préjudice aux règles et procédures propres à chaque service.

L'Autorité de protection des données s'interroge également sur les catégories de données traitées par les "autres destinataires" (§ 103). À cet égard, comme précisé précédemment concernant les §§ 35 et 36 de l'avis, chaque destinataire agit dans le cadre de ses compétences et de ses finalités et traite les données selon ses objectifs sans pour autant devenir des acteurs en matière de terrorisme, extrémisme et processus de radicalisation. Par ailleurs, l'article 24, § 2, précise bien que "Les informations émanant de la carte d'information sont utilisées par le destinataire dans le cadre de ses propres compétences légales, sans que la carte

bedoeld. Mits aan de voorwaarden van dit artikel en van artikel 24 is voldaan, kan het hier gaan om individuele personen. In advies nr. 97/2023 van 16 juni 2023 geeft de Gegevensbeschermingsautoriteit aan dat het beginsel van mededeling op een "behoefte om te kennen"-basis een beoordeling impliceert op basis van (categorieën van) gegevens en niet op basis van een drager als geheel (de informatiekaart) (§ 65). In dat verband kan worden verwezen naar de omschrijving van de informatiekaart, namelijk een kaart die bestaat uit een uittreksel van de inlichtingenfiche, met de persoonsgegevens en informatie die toereikend, ter zake dienend en niet bovenmatig zijn voor de bestemming, voor de opvolging van de entiteiten. Het gaat dus om een informatiekaart "op maat". Er wordt verwezen naar de bespreking bij artikel 14 met betrekking tot het advies van Comité I van 13 juli 2023 betreffende de "need to know" (§ 7).

Een ander voorbeeld: het is mogelijk dat een van de diensten die een leesrecht en een schrijfrecht hebben in de gemeenschappelijke gegevensbank T.E.R., het nodig acht om alle of een deel van de persoonsgegevens over te maken aan een vsw of een school met als doel het vertrek naar Syrië van een jongere die sociaal ontheemd is, te voorkomen. In dit geval moeten de diensten die aan de basis van de informatie liggen, voorafgaand aan deze mededeling evalueren of ze voordelig is voor iedereen, alsook de voorwaarden betreffende deze mededeling, op basis van de in artikel 24 bepaalde modaliteiten.

Om te voorkomen dat er verwarring ontstaat met de term "entiteit" zoals die in artikel 2, 4°, is omschreven en meermaals voorkomt in het ontwerp, is die vervangen door de term "instantie" in het kader van artikel 23.

Er dient te worden gespecificeerd dat deze mededeling ten aanzien van deze ontvangers gebeurt onverminderd de bestaande procedures die hun oorsprong vinden in een wetgevende tekst, zoals een ministerieel besluit, een koninklijk besluit, een wet of een internationaal verdrag. Deze mededeling mag aldus geen afbreuk doen aan de regels en procedures eigen aan iedere dienst.

De Gegevensbeschermingsautoriteit heeft ook vragen bij de categorieën gegevens die worden verwerkt door "andere bestemmingen" (§ 103). In dat verband is het, zoals eerder verduidelijkt met betrekking tot §§ 35 en 36 van het advies, zo dat elke bestemming handelt in het kader van zijn bevoegdheden en doeleinden en dat hij de gegevens verwerkt naargelang zijn doelstellingen, zonder dat hij daarbij actor op het vlak van terrorisme, extremisme en het radicaliseringsproces wordt. Voorts verduidelijkt artikel 24, § 2, het volgende: "De informatie die afkomstig is van de informatiekaart, wordt door de bestemming gebruikt in het kader van zijn eigen

d'information ne soit ni versée au dossier de l'entité ni communiquée à celle-ci.”

Le texte prévoit en outre, dans la mesure où une telle divulgation à des tiers peut compromettre une enquête pénale en cours, qu'il doit donc être possible pour les autorités judiciaires de s'y opposer lorsque la communication des données à caractères personnel et des informations judiciaires peut compromettre l'exercice de l'action publique ou la sécurité de personnes.

L'alinéa 2 précise également l'objet de l'évaluation. Il s'agit d'évaluer au minimum les aspects suivants:

1° la contribution effective des actions de l'autorité ou de l'institution tierce à la prévention ou à la lutte contre le terrorisme et l'extrémisme pouvant mener au terrorisme;

2° le traitement ultérieur qui sera réalisé par l'autorité ou l'institution tierce eu égard à l'exercice de ses compétences et les risques éventuels pour les libertés et droits fondamentaux de la personne concernée;

3° la situation de vulnérabilité de la personne concernée; par exemple, si la personne est mineure ou présente des troubles somatiques et/ou mentaux;

4° le caractère adéquat, pertinent et non excessif des catégories de données communiquées tenant compte du traitement ultérieur.

Dans son avis du 13 juillet 2023, le Comité R a également fait des remarques concernant la communication à des autorités et institutions tierces notamment sur le fait que des règles similaires mais différentes pourraient s'appliquer lorsqu'un autre service de base sera chargé de la communication visée (§ 25). Il faut rappeler ici que chacun travaille selon sa base légale et que les procédures à unifier vis-à-vis de la banque de données commune le sont dans le cadre du présent projet. Quant à la remarque relative au besoin d'en connaître (§ 26), il est renvoyé à ce qui a été développé *supra*. Enfin, le Comité R indique que le projet semble vouloir autoriser les autorités administratives à prendre des décisions sur la base de motifs qui ne sont pas portés à la connaissance de l'intéressé et qui ne figurent pas dans le dossier administratif, ce qui serait contraire à la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs (§ 27). Sur ce point, il faut préciser que la carte d'information contient les mesures qui sont prises à l'égard de l'entité et cette carte ne doit pas être

wettelijke bevoegdheden zonder dat de informatiekaart aan het dossier van de entiteit wordt toegevoegd of aan de entiteit wordt meegedeeld.”

De tekst voorziet ook dat, aangezien dergelijke mededeling aan derden een lopend strafonderzoek in gevaar kan brengen, het dus mogelijk moet zijn voor de gerechtelijke autoriteiten om zich daartegen te verzetten wanneer de mededeling van persoonsgegevens en gerechtelijke informatie de uitoefening van de strafvordering of de veiligheid van personen in het gedrang kunnen brengen.

Het tweede lid verduidelijkt ook wat onder evaluatie wordt verstaan. Zij omvat op zijn minst de volgende aspecten:

1° de effectieve bijdrage van de acties van de derde overheid of de derde instelling tot het voorkomen of bestrijden van terrorisme en van extremisme dat tot terrorisme kan leiden;

2° de verdere verwerking die zal worden verricht door de derde overheid of de derde instelling, in het licht van de uitoefening van haar bevoegdheden en de eventuele risico's voor de fundamentele rechten en vrijheden van de betrokken persoon;

3° de kwetsbare situatie van de betrokken persoon, bijvoorbeeld wanneer de betrokkene minderjarig is of te kampen heeft met lichamelijke of mentale problemen;

4° het toereikende, ter zake dienende en niet overmatige karakter van de categorieën van meegedeelde gegevens, rekening houdend met de verdere verwerking.

In het advies van 13 juli 2023 heeft Comité I ook opmerkingen gemaakt over de mededeling aan derde overheden en instellingen, met name over het feit dat er vergelijkbare maar verschillende regels van toepassing kunnen zijn als een andere basisdienst verantwoordelijk is voor deze communicatie (§ 25). Er zij op gewezen dat iedereen werkt volgens zijn wettelijke basis en dat de eenvormigheidsprocedures ten opzichte van de gemeenschappelijke gegevensbank binnen dit ontwerp kaderen. De opmerking rond de “need to know” (§ 26) is reeds hierboven uiteengezet. Tot slot geeft Comité I aan dat het ontwerp de administratieve overheden lijkt te willen machtigen om beslissingen te nemen op basis van motieven die niet ter kennis van de betrokkene worden gebracht en die niet in het administratief dossier zijn opgenomen, wat in strijd zou zijn met de wet van 29 juli 1991 betreffende de uitdrukkelijke motivering van de bestuurshandelingen. Daarover moet worden verduidelijkt dat de informatiekaart maatregelen bevat die worden genomen ten aanzien van de entiteit en dat

accessible à l'entité. Le but de la carte d'information est d'éviter que l'autorité administrative ne prennent des mesures contradictoires par rapport à celles qui ont été discutées en TFL. Ce qui sert à la motivation de la décision de l'autorité administrative, c'est l'évaluation de la menace qui, elle, peut être versée au dossier de l'entité (art. 27).

Suite à l'avis du C.O.C. du 20 juin 2023, l'article 23 (ancien art. 24) est complété avec un nouvel alinéa prévoyant qu'une liste de ces communications à des autorités tierces est tenue par le responsable opérationnel à l'intention des autorités de contrôle, avec la possibilité de retrouver l'évaluation faite pour chaque transfert.

Art. 24

Cet article reprend le principe de la carte d'information contenu à l'article 11, § 1^{er} et § 2, alinéas 1 et 2, de l'arrêté royal "TF" et de l'arrêté royal "PH". Cependant, dans un objectif de précision, l'article 24 prévoit désormais que la carte d'information ne peut pas être versée au dossier de l'entité validée et communiquée à l'entité concernée. La carte d'information est destinée aux autorités susceptibles de prendre des mesures à l'égard des entités validées de la banque de données commune T.E.R., dans le but d'éviter la prise de mesures incohérentes entre elles. Verser la carte d'information au dossier signifie donner un accès direct aux informations/données enregistrées dans la banque de données commune T.E.R. Or, la carte d'information contient les mesures de suivi qui ne doivent pas être connues de l'entité validée concernée (ex. enquête judiciaire ou de renseignement, surveillance discrète) au risque d'entraver une enquête. Outre les mesures de suivi, la carte d'information peut également contenir des informations qu'il n'est pas pertinent de communiquer à l'entité validée concernée. Exemples: les services intéressés dans le suivi de la personne (ex. la PJF d'Anvers), la date du début du suivi.

En outre, la communication vers le destinataire doit se faire de manière sécurisée. Il convient de prendre les mesures raisonnables pour empêcher la divulgation de données à des personnes n'ayant pas de motifs légitimes pour en prendre connaissance.

de l'entité geen toegang tot die kaart moet hebben. Doel van de informatiekaart is te voorkomen dat de administratieve overheden tegenstrijdige maatregelen nemen ten opzichte van de maatregelen die in de LTF zijn besproken. Wat dient ter motivering van de beslissing van de administratieve overheid, is de dreigingsevaluatie, die aan het dossier van de entiteit mag worden toegevoegd (art. 27).

Ingevolge het advies van 20 juni 2023 van het COC wordt artikel 23 (oud artikel 24) aangevuld met een nieuw lid waarin staat dat er door de operationeel verantwoordelijke, ten behoeve van de toezichhoudende overheden, een lijst van dergelijke mededelingen aan derde overheden bijhoudt, met de mogelijkheid om voor elke doorgifte de opgemaakte evaluatie desbetreffend terug te vinden.

Art. 24

Dit artikel herneemt het beginsel van de informatiekaart vervat in artikel 11, § 1 en § 2, eerste en tweede lid, van het koninklijk besluit "TF" en het koninklijk besluit "HP". Ter verduidelijking is in artikel 24 voortaan echter bepaald dat de informatiekaart niet aan het dossier van de gevalideerde entiteit mag worden toegevoegd en niet aan de betrokken entiteit mag worden meegedeeld. De informatiekaart is bedoeld voor gebruik door de autoriteiten die maatregelen kunnen nemen ten aanzien van de gevalideerde entiteiten van de gemeenschappelijke gegevensbank T.E.R., teneinde te voorkomen dat zij onderling tegenstrijdige maatregelen nemen. Het opnemen van de informatiekaart in het dossier betekent dat rechtstreeks toegang wordt verleend tot de informatie/gegevens die in de gemeenschappelijke gegevensbank T.E.R. zijn opgeslagen. De informatiekaart bevat vervolmaatregelen die niet bekend hoeven te zijn bij de betrokken gevalideerde entiteit (bijvoorbeeld gerechtelijk of inlichtingenonderzoek, onopvallende observatie) met het risico dat een onderzoek wordt belemmerd. Naast vervolmaatregelen kan de informatiekaart ook informatie bevatten die niet relevant is voor de betrokken gevalideerde entiteit. Voorbeelden: de diensten die betrokken zijn bij het toezicht op de persoon (bijvoorbeeld FGP Antwerpen), de datum van het begin van het toezicht.

Bovendien moet de mededeling naar de ontvanger op een veilige manier gebeuren. Er moeten redelijke maatregelen worden genomen om te voorkomen dat gegevens worden verstrekt aan personen die geen legitieme redenen hebben om toegang tot die gegevens te krijgen.

Les modalités de communication des données à caractère personnel et des informations à une autorité ou une institution tierce visée à l'article 23, déterminent que:

— seuls les services de base peuvent communiquer des données;

— la communication ne concerne que les données des entités qui remplissent les critères pour être considérées comme *foreign terrorist fighters*, *homegrown terrorist fighters*, extrémistes potentiellement violents, personnes condamnées pour terrorisme ou propagandistes de haine;

— les données communiquées sont celles de la carte d'information ou d'une partie de celle-ci.

Cet article énonce le principe général selon lequel aucun destinataire d'une carte d'information ne peut verser celle-ci dans un dossier sur base duquel une décision administrative est prise concernant la personne visée. En effet, il faut éviter que les données et informations de ce document ne soit divulguées à des personnes ou organismes au sens large ayant accès au dossier et qui ne sont pas directement liés à la lutte contre le terrorisme et que le mécanisme de protection des données gérées au sein de la banque de données commune T.E.R. ne puisse être contourné par une procédure administrative.

Art. 25

L'article 25 reprend le contenu de l'article 11, § 2, alinéas 3 et 4, de l'arrêté royal "TF" et de l'arrêté royal "PH". Sur le fond, aucune modification n'a été apportée.

Cet article concerne la communication des données à caractère personnel et des informations extraites de la carte d'informations sous forme de listes à d'autres services ou institutions.

La notion de liste répond à l'acceptation commune de ce terme: une énumération de données personnelles (ex.: date de naissance, numéro d'e-ID, ...) se rapportant à plusieurs personnes. La liste se différencie de la carte d'information dans le sens que cette dernière ne concerne qu'une seule personne et contient un plus grand nombre de données propres à cette personne. Une liste contient au minimum les données anonymisées des entités (statistiques) et au maximum les données à caractère personnel et informations des cartes d'information relatives à celles-ci.

De nadere regels inzake de mededeling van de persoonsgegevens en informatie aan een derde overheid of een derde instelling bedoeld in artikel 23, bepalen dat:

— enkel de basisdiensten gegevens mogen meedelen;

— de mededeling enkel de gegevens betreft van entiteiten die beantwoorden aan de criteria om te worden beschouwd als *foreign terrorist fighter*, *homegrown terrorist fighter*, potentieel gewelddadige extremist, terrorismeveroordeelde of haatpropagandist;

— de meegedeelde informatie, informatie betreft van de informatiekaart of van een gedeelte ervan.

Dit artikel bevat het algemene principe volgens hetwelk geen enkele bestemming van een informatiekaart deze kaart in een dossier mag voegen op basis waarvan een administratieve beslissing wordt genomen met betrekking tot de betrokken persoon. Men dient namelijk te verhinderen dat de gegevens en de informatie van dit document verstrekt zouden worden aan personen of organismen in brede zin die toegang hebben tot het dossier en die niet rechtstreeks verbonden zijn aan de strijd tegen het terrorisme en dat het beschermingsmechanisme van gegevens die in de gemeenschappelijke gegevensbank T.E.R. beheerd worden omzeild kan worden door een administratieve procedure.

Art. 25

Artikel 25 herneemt de inhoud van artikel 11, § 2, derde en vierde lid, van het koninklijk besluit "TF" en het koninklijk besluit "HP". Inhoudelijk werden er geen wijzigingen aangebracht.

Dit artikel betreft de mededeling aan andere diensten of instellingen van persoonsgegevens en informatie die in de vorm van lijsten uit de informatiekaart worden gehaald.

Het begrip "lijst" moet begrepen worden in de gebruikelijke betekenis van het woord: een opsomming van persoonsgegevens (bijvoorbeeld: geboortedatum, eID-nummer, ...) die betrekking heeft op meerdere personen. De lijst verschilt van de informatiekaart die slechts één persoon betreft en die meer gegevens bevat over deze persoon. Een lijst bevat minstens de geanonimiseerde gegevens van entiteiten (statistiek) en hoogstens de persoonsgegevens en informatie van de informatiekaarten die erop betrekking hebben.

La communication par les services de bases des données à caractère personnel ou informations, sous formes de listes, extraites de cartes d'information, relative aux entités validées, à d'autres services ou institutions n'est donc pas autorisée, sauf dans les cas prévus à l'article 23, c'est-à-dire lorsque le gestionnaire, le responsable opérationnel et les services de base estiment que la communication est nécessaire pour une finalité précise dont est chargé le destinataire en question. En effet, la communication ne peut être effectuée qu'avec une finalité déterminée qui s'inscrit dans le cadre des missions légales du destinataire en question (par exemple, pour la mise à jour de la banque de données que gère le Ministère public une liste des nouvelles entités et des entités supprimées est adressée aux magistrats spécialisés). Les listes ne peuvent en aucun cas être utilisées à d'autres fins. Finalement, les listes ne peuvent pas être conservées pour une durée excédant celle nécessaire à la réalisation de la finalité pour laquelle elles sont obtenues.

Par cette limitation, l'objectif est d'éviter que des listes de données à caractère personnel ne soient diffusées de manière inopportune, pour des finalités qui ne le justifient pas. En effet, le fait d'être repris sur une telle liste entraîne de lourdes conséquences pour les entités concernées.

Il faut noter que par rapport au texte existant, le libellé a été précisé. L'article actuel prévoit en effet que "Ce traitement est effectué par un membre du personnel titulaire d'une habilitation de sécurité "secret".". Le traitement visé consiste en réalité l'extraction des listes de données à caractère personnel et d'informations de la carte d'information relative aux entités et ce, exclusivement pour un traitement interne. Les mots "ce traitement" sont dès lors remplacés par les mots "cette extraction". Il faut préciser que dans la mesure où celui qui effectue l'extraction a un droit de lecture et d'écriture dans la banque de données commune T.E.R., il doit dès lors avoir une habilitation de sécurité de niveau "secret". En revanche, celui qui reçoit l'information extraite, ne doit pas d'office avoir cette habilitation de niveau "secret".

Dans son avis du 13 juillet 2023, le Comité R estime que les finalités de l'extraction et de la communication à des tiers de listes ne sont pas suffisamment déterminées (§ 28). Or, les finalités sont déterminées en fonction des missions légales du destinataire, comme cela est indiqué dans l'article 25, § 2. Ces listes sont destinées à des partenaires qui ne sont pas les partenaires "naturels" de la banque de données commune. Il n'est dès lors pas

De mededeling door de basisdiensten van persoonsgegevens of informatie, in de vorm van lijsten, afkomstig uit de informatiekaarten en met betrekking tot gevalideerde entiteiten, aan andere diensten of instellingen wordt dan ook niet toegestaan, met uitzondering van de gevallen zoals voorzien in artikel 23, zijnde indien de beheerder, de operationeel verantwoordelijke en de basisdiensten, menen dat de mededeling noodzakelijk is voor een welbepaald doel waarmee de betrokken bestemming belast werd. Daarnaast mag de mededeling van een of meerdere lijsten enkel gebeuren omwille van een welbepaald doel dat kadert in de wettelijke opdrachten van de betrokken bestemming (bijvoorbeeld, voor het bijwerken van de door het openbaar ministerie beheerde gegevensbank wordt een lijst van nieuwe en geschrapte entiteiten aan de gespecialiseerde magistraten toegezonden). Deze lijsten mogen onder geen beding gebruikt worden voor andere doelstellingen. Ten slotte mogen de lijsten niet langer bewaard worden dan nodig is voor de verwezenlijking van de doelstelling waarvoor ze worden verkregen.

Deze beperking heeft als doel te vermijden dat lijsten met persoonsgegevens op een ongepaste wijze verspreid worden voor doeleinden die dit niet rechtvaardigen. Opgenomen worden op een dergelijke lijst heeft immers zware gevolgen voor de betrokken entiteiten.

Er wordt op gewezen dat de formulering ten opzichte van de bestaande tekst werd verduidelijkt. Het huidige artikel bepaalt immers dat "Deze verwerking gebeurt door een personeelslid dat houder is van een veiligheidsmachtiging van het niveau "geheim".". De verwerking in kwestie bestaat in feite uit de extractie van lijsten van persoonsgegevens en informatie van de informatiekaart betreffende de entiteiten, en dit uitsluitend voor een interne verwerking. De woorden "deze verwerking" worden derhalve vervangen door de woorden "deze extractie". Er moet worden verduidelijkt dat, aangezien degene die de extractie uitvoert een leesrecht en een schrijfrecht heeft in de gemeenschappelijke gegevensbank T.E.R., die persoon derhalve moet beschikken over een veiligheidsmachtiging van het niveau "geheim". Degene die de geëxtraheerde informatie ontvangt, moet daarentegen niet per definitie beschikken over die machtiging van het niveau "geheim".

In het advies van 13 juli 2023 is Comité I van mening dat de doeleinden van het opvragen van lijsten en het meedelen ervan aan derden niet voldoende zijn bepaald (§ 28). De doeleinden worden evenwel, zoals aangegeven in artikel 25, § 2, bepaald naargelang de wettelijke opdrachten van de ontvanger. Die lijsten zijn bestemd voor partners die niet de "natuurlijke" partners van de gemeenschappelijke gegevensbank zijn. Het is

possible d'indiquer comment ces listes seront utilisées vu que cela dépendra du destinataire et de ses missions légales. La finalité précise sera déterminée au moment de la communication.

Ensuite, le Comité R indique qu'un mécanisme de mise à jour des listes est nécessaire (§ 29). La banque de données commune est un outil dynamique et dans le cadre de l'extraction de listes, une communication des mises à jour est faite de façon périodique. Cela dépend également du contexte dans lequel la communication de liste a été faite. En outre, il appartient au destinataire de la liste de vérifier que sa liste est à jour lorsqu'il prend des mesures ultérieurement.

Art. 26

Suite à l'avis n° 97/2023 du 16 juin 2023 de l'Autorité de protection des données (§ 67), cet article prévoit la communication de la carte d'information au bourgmestre.

Vu les compétences du bourgmestre en matière de sécurité telles que légalement définies dans la nouvelle loi communale, celui-ci doit disposer des informations nécessaires afin d'exercer son rôle dans le domaine de la prévention en matière de terrorisme. En tant qu'autorité en matière de police administrative, il doit également être tenu au courant du suivi concret de certaines entités validées liées à sa commune.

Le bourgmestre devra donc être informé lorsqu'une entité validée, dont les activités ont des effets perceptibles dans sa commune ou qui a établi sa résidence ou son domicile dans sa commune, la fréquente régulièrement, y organise ou planifie d'y organiser une ou plusieurs activités, est suivie dans la banque de données commune T.E.R.

Cette information au bourgmestre est transmise au moyen de la carte d'information.

Sous sa responsabilité, le bourgmestre pourra partager ces données et informations avec les différents acteurs locaux qui ont la nécessité de prendre connaissance de celles-ci pour l'exercice de leurs missions légales, et donc dans le respect des principes d'adéquation, de pertinence et du caractère non excessif.

Ce partage d'informations ne peut bien entendu pas mettre en péril les missions opérationnelles qui découlent de l'exploitation des données et informations gérées dans la banque de données commune T.E.R.

derhalve niet mogelijk om aan te geven hoe die lijsten zullen worden gebruikt, aangezien dat zal afhangen van de ontvanger en zijn wettelijke opdrachten. Het precieze doeleinde wordt bepaald wanneer ze worden meegedeeld.

Vervolgens geeft Comité I aan dat er een mechanisme nodig is voor het bijwerken van de lijsten (§ 29). De gemeenschappelijke gegevensbank is een dynamische tool, en in het kader van de opvraging van de lijsten, worden de bijwerkingen periodiek meegedeeld. Dat hangt eveneens af van de context waarbinnen de lijst werd meegedeeld. Bovendien is het de taak van de ontvanger van de lijst om na te gaan of zijn lijst up-to-date is wanneer hij later maatregelen neemt.

Art. 26

Ingevolge advies nr. 97/2023 van 16 juni 2023 van de Gegevensbeschermingsautoriteit (§ 67) bepaalt dit artikel de mededeling van de informatiekaart aan de burgemeester.

Gelet op de bevoegdheden van de burgemeester op het gebied van veiligheid zoals wettelijk bepaald in de nieuwe gemeentewet, moet deze over de noodzakelijke informatie beschikken om zijn rol uit te oefenen op het vlak van het voorkomen van terrorisme. Als overheid van bestuurlijke politie moet hij tevens op de hoogte gehouden worden van de concrete opvolging van sommige aan zijn gemeente verbonden gevalideerde entiteiten.

De burgemeester zal dus in kennis moeten worden gesteld wanneer een entiteit gevalideerde, waarvan de activiteiten zichtbare effecten hebben in zijn gemeente of die zijn woonplaats gevestigd heeft in zijn gemeente, deze regelmatig bezoekt, er één of meerdere activiteiten organiseert of plant te organiseren, wordt opgevolgd in de gemeenschappelijke gegevensbank T.E.R.

Deze in kennisstelling van de burgemeester gebeurt door middel van de informatiekaart.

De burgemeester zal deze gegevens en informatie, onder zijn verantwoordelijkheid, kunnen delen met de verschillende lokale actoren die genoodzaakt zijn om daarvan kennis te nemen voor de uitoefening van hun wettelijke opdrachten, in dus met inachtneming van de principes van toereikendheid, relevantie en de niet-bovenmatige aard.

Deze informatiedeling mag de operationele opdrachten die voortvloeien uit de exploitatie van de gegevens en informatie beheerd in de gemeenschappelijke gegevensbank T.E.R. uiteraard niet in gevaar brengen.

S'il existe un doute quant au fait de mettre en péril une mission opérationnelle, le bourgmestre prendra toujours contact avec le chef de corps du service de police qui lui a transmis la carte d'information.

En ce qui concerne l'information du bourgmestre, il faut donc distinguer deux moments. D'une part, l'information du bourgmestre par la voie du chef de Corps dès la création d'une entité, et d'autre part, l'information du bourgmestre au moyen de la carte d'information pour le suivi de l'entité validée. Le premier moment a pour objectif d'informer le plus rapidement possible le bourgmestre même si les informations disponibles ne sont pas encore complètes. Le second moment donne au bourgmestre des informations dont le contenu est plus développé pour qu'il puisse prendre les mesures qui relèvent de ses compétences.

Dans son avis précité, l'Autorité de protection des données s'interroge sur la qualité en vertu de laquelle le bourgmestre reçoit l'information (§§ 67 à 73). Cette communication est bien entendu en lien avec les missions qui lui sont attribuées en sa qualité d'autorité en matière de police administrative par l'article 133, alinéa 3, de la nouvelle loi communale. Par ailleurs, la mise en place des CSIL-R avait pour but de pallier l'absence d'une structure existante permettant d'échanger des informations, il n'était pas question de régler la communication entre le bourgmestre et son chef de corps.

Art. 27

L'objectif de la banque de données commune n'est pas seulement d'améliorer le partage de données, mais aussi d'encadrer la prise de mesures, concertées au sein des plateformes prévues. Les services qui ont un droit de lecture et un droit d'écriture dans la banque de données commune T.E.R. peuvent fonder leurs décisions administratives sur l'évaluation de la menace fournie par l'OCAM, et introduite dans la banque de données commune T.E.R. Pour éviter une double charge de travail pour les services qui alimentent la banque de données, il leur est donc possible d'imprimer l'évaluation de l'OCAM avec entête officielle, date et signature du directeur de l'OCAM.

Il s'est avéré dans la pratique que définir les conditions d'utilisation de la fiche de renseignement et la carte d'information n'était pas suffisant dans la mesure où l'évaluation de la menace réalisée par l'OCAM pour chaque entité validée – qui se fonde notamment sur les données de la fiche de renseignement – était également mise à disposition des utilisateurs de la banque

Wanneer twijfel bestaat over het in gevaar brengen van een operationele opdracht, moet de burgemeester altijd contact opnemen met de korpschef van de politiedienst die hem de informatiekaart overmaakte.

Wat het informeren van de burgemeester betreft, moet er dus een onderscheid worden gemaakt tussen twee momenten. Het informeren van de burgemeester via de korpschef zodra er een entiteit is gecreëerd enerzijds en het informeren van de burgemeester door middel van de informatiekaart voor de opvolging van de gevalideerde entiteit anderzijds. Bij het eerste moment is het de bedoeling om de burgemeester zo snel mogelijk te informeren, zelfs als de beschikbare informatie nog niet volledig is. Bij het tweede moment wordt aan de burgemeester informatie verstrekt waarvan de inhoud meer ontwikkeld is zodat hij de maatregelen kan nemen waarvoor hij bevoegd is.

In het voornoemde advies heeft de Gegevensbeschermingsautoriteit vragen bij de hoedanigheid op grond waarvan een burgemeester de informatie ontvangt (§§ 67 tot 73). Die mededeling houdt uiteraard verband met de hem toegekende opdrachten in zijn hoedanigheid van bestuurlijke politieautoriteit op grond van artikel 133, derde lid, van de nieuwe gemeentewet. Overigens was het doel van de invoering van de LIVC-R's om het gebrek aan een bestaande informatie-uitwisselingsstructuur te verhelpen en was het niet de bedoeling om de communicatie tussen burgemeester en korpschef te regelen.

Art. 27

Het doel van de gemeenschappelijke gegevensbank is niet enkel het verbeteren van het delen van gegevens, maar ook het bieden van een omkadering voor het nemen van maatregelen overlegd binnen de hiervoor voorziene platformen. De diensten die een leesrecht en een schrijfrecht hebben in de gemeenschappelijke gegevensbank T.E.R. kunnen hun administratieve beslissingen steunen op de evaluatie van de dreiging verstrekt door het OCAD en ingevoerd in de gemeenschappelijke gegevensbank T.E.R. Om een dubbele werklast te vermijden voor de diensten die de gegevensbank voeden, is het voor hen dus mogelijk om de evaluatie van het OCAD, met officiële hoofding, datum en handtekening van de directeur van het OCAD, te printen.

In de praktijk is gebleken dat het niet voldoende was om de gebruiksvoorwaarden van de inlichtingenfiche en de informatiekaart te bepalen, aangezien de dreigings-evaluatie die het OCAD voor elke gevalideerde entiteit uitvoert – die inzonderheid gebaseerd is op de gegevens van de inlichtingenfiche – ook ter beschikking werd gesteld aan de gebruikers van de gemeenschappelijke

de données commune T.E.R. et que par conséquent, il convenait aussi d'en encadrer l'utilisation.

Ainsi, l'évaluation de la menace peut être utilisée par les services de base et les services partenaires dans le cadre de leurs propres compétences légales et conformément aux finalités de l'article 5, alinéa 2. L'évaluation de la menace peut en outre être versée au dossier de l'entité, moyennant la validation de celle-ci par l'OCAM. Dans un souci d'effectivité, la validation devrait intervenir dans un délai de maximum deux semaines ou en cas d'urgence, dans les 48 heures. Cette utilisation de l'évaluation de la menace et son versement au dossier de l'entité peuvent faire l'objet d'un protocole d'accord entre les services concernés et l'OCAM, en tant qu'organe compétent pour l'évaluation de la menace. Cette validation permet à l'OCAM de s'assurer que l'évaluation de la menace qui sera versée au dossier de l'entité par le service partenaire a bien été mise à jour. Cette actualisation a lieu au minimum 2 fois par an.

Dès lors que l'évaluation de la menace est versée au dossier, la personne peut bien entendu en prendre connaissance à travers les procédures contentieuses ou judiciaires en cours, qui impliquent une communication du dossier. Elle en prendra connaissance directement ou via son avocat. À titre illustratif, si une maison de Justice demande et reçoit une évaluation de la menace à propos d'une personne, elle peut verser cette évaluation au dossier de l'entité, lequel sera selon les règles en vigueur transmis au juge du fond.

Art. 28

L'article 28 reprend d'une part le principe de l'article 15, § 1^{er}, de l'arrêté royal "TF" et de l'arrêté royal "PH" et d'autre part, celui de l'article 44/11/3^{quinties} de la loi sur la fonction de police.

Il concerne l'échange des données à caractère personnel et informations de la banque de données commune T.E.R. sur le plan international.

Etant donné que les différents partenaires clefs d'une banque de données commune ont chacun leurs propres canaux d'échange d'informations avec leurs partenaires étrangers, les principes y relatifs sont également repris dans cet article.

Cependant, l'article ne prévoit plus de communication par l'OCAM des données à caractère personnel et informations de la banque de données commune T.E.R. avec ses homologues étrangers. En effet, l'OCAM ne peut pas communiquer de renseignement à l'étranger vu qu'il n'est pas un organe opérationnel. Il peut seulement

gegevensbank T.E.R. en het gebruik ervan bijgevolg ook moest worden gereguleerd.

Zo kan de dreigingsevaluatie door de basisdiensten en de partnerdiensten worden gebruikt in het kader van hun eigen wettelijke bevoegdheden en overeenkomstig de doeleinden van artikel 5, tweede lid. De dreigingsevaluatie mag ook aan het dossier van de entiteit worden toegevoegd indien deze door het OCAD is gevalideerd. Om doeltreffend te zijn moet de validatie binnen een termijn van maximaal twee weken plaatsvinden of, in dringende gevallen, binnen 48 uur. Voor dit gebruik van de dreigingsevaluatie en de opname ervan in het dossier van de entiteit kan een protocolakkoord worden opgesteld tussen de betrokken diensten en het OCAD, als bevoegde instantie voor de dreigingsevaluatie. Met deze validatie kan het OCAD ervoor zorgen dat de dreigingsevaluatie dat door de partnerdienst in het dossier van de entiteit wordt opgenomen, is geactualiseerd. Deze bijwerking vindt ten minste tweemaal per jaar plaats.

Zodra de dreigingsevaluatie in het dossier is opgenomen, kan de persoon er uiteraard kennis van nemen via lopende rechtszaken of gerechtelijke procedures, waarbij het dossier wordt meegedeeld. Hij of zij zal er rechtstreeks of via zijn of haar advocaat kennis van nemen. Ter illustratie: als een Justitiehuis een dreigingsevaluatie over een persoon vraagt en ontvangt, kan het deze evaluatie in het dossier van de entiteit plaatsen, dat volgens de geldende regels aan de feitenrechter zal worden toegezonden.

Art. 28

Artikel 28 wordt het principe hernomen van artikel 15, § 1, van het koninklijk besluit "TF" en van het koninklijk besluit "HP", alsmede dat van artikel 44/11/3^{quinties} van de wet op het politieambt.

Het betreft de uitwisseling van persoonsgegevens en informatie uit de gemeenschappelijke gegevensbank T.E.R. op internationaal niveau.

Aangezien de verschillende sleutelpartners van een gemeenschappelijke gegevensbank elk hun eigen kanalen voor informatie-uitwisseling met hun buitenlandse partners hebben, worden de desbetreffende principes eveneens in dit artikel hernomen.

In het artikel wordt echter niet langer bepaald dat het OCAD persoonsgegevens en informatie uit de gemeenschappelijke gegevensbank T.E.R. aan zijn buitenlandse tegenhangers meedeelt. Het OCAD kan immers geen inlichtingen aan het buitenland meedelen aangezien het geen operationeel orgaan is. Het kan enkel informatie van

recevoir de l'information de ses services d'appui conformément à l'article 6 de la loi du 10 juillet 2006 "relative à l'analyse de la menace" et communiquer ses évaluations de la menace conformément à l'article 10 de la même loi, article 10 qui ne prévoit pas la communication des évaluations à un organisme étranger. L'invocation de l'article 8, alinéa 1^{er}, 3^o de la loi OCAM dans l'article 15, § 1^{er}, de l'arrêté royal "TF" et de l'arrêté royal "PH" est donc erronée pour fonder une compétence de divulgation que l'OCAM n'a pas.

Au niveau du libellé, il faut préciser que dans l'article 28, § 2, les mots "conformément à l'article 44/11/13 de la loi sur la fonction de police" remplacent les mots de l'article 15, § 2, de l'AR "TF" "conformément aux dispositions de l'arrêté royal du 30 octobre 2015 relatif aux conditions afférentes à la communication des données à caractère personnel et des informations des services de police belges aux membres d'Interpol et à Interpol et du chapitre 1^{er}/1^{er} de la loi du 9 décembre 2004 sur la transmission policière internationale de données à caractère personnel et d'informations à finalité judiciaire, l'entraide judiciaire internationale en matière pénale et modifiant l'article 90^{ter}, du Code d'instruction criminelle."

En outre, afin d'envisager toutes les situations possibles, il est également ajouté que les données à caractère personnel et les informations de la banque de données commune T.E.R. peuvent être communiquées aux autorités judiciaires étrangères.

En ce qui concerne le cas particulier des étrangers, il faut rappeler qu'il existe des obligations réglementaires pour certaines catégories d'étrangers.

Ainsi, il existe une interdiction de communiquer certaines informations, dans le cadre de l'examen de cas individuels, à savoir:

- les informations concernant une demande de protection internationale, ou le fait qu'une demande a été présentée (par ex. une demande de statut de réfugiés ou de statut conféré par la protection subsidiaire) ou le fait qu'une demande a été présentée auprès de l'auteur ou des auteurs présumés de persécutions ou d'atteintes graves;

- obtenir des informations d'une manière telle que l'auteur (ou les auteurs) présumé(s) de persécutions ou d'atteintes graves à l'encontre du demandeur soi(en)t directement informé(s) qu'une demande a été présentée par le demandeur en question, et que l'intégrité physique de ce dernier ou des personnes à sa charge, ou la liberté

zijn steundiensten ontvangen overeenkomstig artikel 6 van de wet van 10 juli 2006 betreffende de analyse van de dreiging, en het kan zijn dreigingsevaluaties meedelen overeenkomstig artikel 10 van diezelfde wet, dat niet bepaalt dat de evaluaties aan een buitenlands orgaan worden meegedeeld. Het is dus niet juist om artikel 8, eerste lid, 3^o, van de OCAD-wet in artikel 15, § 1, van het koninklijk besluit "TF" en van het koninklijk besluit "HP" aan te voeren ten grondslag van een bekendmakingsbevoegdheid die het OCAD niet heeft.

Wat de formulering betreft, dient te worden verduidelijkt dat in artikel 28, § 2, de woorden "in overeenstemming met artikel 44/11/13 van de wet op het politieambt" de woorden van artikel 15, § 2 van het koninklijk besluit "TF" "in overeenstemming met de bepalingen van het koninklijk besluit van 30 oktober 2015 betreffende de voorwaarden verbonden aan de mededeling van persoonsgegevens en informatie door de Belgische politiediensten aan de leden van Interpol en Interpol en het hoofdstuk I/1 van de wet van 9 december 2004 betreffende de internationale politieke verstrekking van gegevens van persoonlijke aard en informatie met gerechtelijke finaliteit, de wederzijdse internationale rechtshulp in strafzaken en tot wijziging van artikel 90^{ter} van het Wetboek van strafvordering." vervangen.

Om alle mogelijke situaties te bestrijken, wordt bovendien toegevoegd dat persoonsgegevens en informatie in de gemeenschappelijke gegevensbank T.E.R. aan buitenlandse gerechtelijke autoriteiten kunnen worden meegedeeld.

Wat het specifieke geval van vreemdelingen betreft, zij eraan herinnerd dat er voor bepaalde categorieën van vreemdelingen wettelijke verplichtingen bestaan.

Zo geldt er een verbod op openbaarmaking van bepaalde informatie in het kader van het onderzoek van individuele gevallen, namelijk:

- informatie betreffende een verzoek om internationale bescherming of het feit dat een verzoek is ingediend (i.e. een verzoek om vluchtelingenstatus of subsidiaire beschermingsstatus) of het feit dat een verzoek is ingediend tegen de vermeende actor(en) van de vervolging of ernstige schade;

- informatie in te winnen op zodanige wijze dat de vermeende actor(en) van de vervolging of ernstige schade jegens de verzoeker er rechtstreeks van in kennis wordt (worden) gesteld dat door de betrokken verzoeker een verzoek is ingediend, en dat de fysieke integriteit van de verzoeker of de te zijnen laste komende personen,

et la sécurité des membres de sa famille qui séjournent encore dans son pays d'origine, soient compromises.

Cette interdiction est imposée aux États membres par l'article 30 de la directive 2013/32/UE du Parlement européen et du Conseil du 26 juin 2013 relative à des procédures communes pour l'octroi et le retrait de la protection internationale (refonte).

L'avis 73.442/2 du Conseil d'État du 7 juin 2023 a été suivi concernant cet article. L'habilitation au Roi pour déterminer les modalités de la communication est donc supprimée. En effet, ces communications vis-à-vis de l'étranger doivent suivre les règles issues soit de la loi sur la fonction de police soit de la loi des services de renseignement et de sécurité qui prévoient ces modalités.

Dans son avis n° 97/2023 du 16 juin 2023, l'Autorité de protection des données s'interroge sur cet article (§ 111). À cet égard, rappelons que l'objectif de la banque de données commune n'est pas d'avoir une dissémination des données et des informations qui y figurent. L'article 28 détermine clairement dans quels cas s'effectue la communication internationale: seul un service de base peut communiquer à l'international les données à caractère personnel et informations de la banque de données commune T.E.R. et ce, dans le respect pour chacun de ces services de la législation qui le concerne (§§ 2 et 3 de l'article 28). Chaque service de base garde ses canaux privilégiés de communication, et cette communication elle-même est soumise à sa propre réglementation.

Dans son avis du 13 juillet 2023, le Comité R recommande, conformément à sa note n° 2023.300, de tenir compte, dans la définition des exigences applicables aux flux transfrontières de données à caractère personnel les règles de la Convention 108 + du Conseil de l'Europe, signé par la Belgique le 10 octobre 2018 (§ 30). L'auteur du projet constate cependant que ces règles de la Convention 108 + s'appliquent à l'ensemble des traitements de données à caractère personnel et pas uniquement aux traitements dans la banque de données commune T.E.R. Il conviendra donc de tenir compte de ces règles de la Convention 108 + dans le cadre de la révision générale de la loi du 30 juillet 2018 relative à la protection des données à caractère personnel et non pas séparément dans le présent projet.

dan wel de vrijheid en veiligheid van zijn nog in het land van herkomst verblijvende familieleden in gevaar zou worden gebracht.

Dit verbod wordt door artikel 30 van de Richtlijn 2013/32/EU van het Europees Parlement en de Raad van 26 juni 2013 betreffende gemeenschappelijke procedures voor de toekenning en intrekking van de internationale bescherming (herschikking) aan de lidstaten opgelegd.

Advies nr. 73.442/2 van 7 juni 2023 van de Raad van State is voor dit artikel gevolgd. De machtiging aan de Koning om de nadere regels voor het creatierecht te bepalen, wordt aldus geschrapt. Dergelijke mededelingen naar het buitenland moeten namelijk de regels volgen hetzij uit de wet op het politieambt, hetzij uit de wet houdende regeling van de inlichtingen- en veiligheidsdiensten, waarin in die nadere regels is voorzien.

In advies nr. 97/2023 van 16 juni 2023 heeft de Gegevensbeschermingsautoriteit vragen bij dit artikel (§ 111). In dat opzicht moet erop worden gewezen dat het niet de bedoeling van de gemeenschappelijke gegevensbank is dat de gegevens en informatie erin worden verspreid. In artikel 28 wordt duidelijk bepaald in welke gevallen de internationale mededeling gebeurt: enkel een basisdienst mag persoonsgegevens en informatie van de gemeenschappelijke gegevensbank T.E.R. meedelen aan het buitenland, en zulks met eerbiediging voor elk van deze diensten van de desbetreffende wetgeving (§§ 2 en 3 van artikel 28). Elke basisdienst behoudt zijn geprivilegieerde communicatiekanalen, en die mededeling zelf is onderworpen aan zijn eigen regelgeving.

In het advies van 13 juli 2023 beveelt Comité I, overeenkomstig zijn nota nr. 2023.300, aan om bij het bepalen van de vereisten die van toepassing zijn op grensoverschrijdende stromen van persoonsgegevens, rekening te houden met de regels van Verdrag 108+ van de Raad van Europa, ondertekend door België op 10 oktober 2018 (§ 30). De auteur van het ontwerp constateert echter dat die regels van Verdrag 108+ van toepassing zijn op alle verwerkingen van persoonsgegevens en niet enkel op de verwerkingen binnen het kader van de gemeenschappelijke gegevensbank T.E.R. Bijgevolg zal er rekening moeten worden gehouden met die regels van Verdrag 108+ bij de algemene herziening van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, en niet afzonderlijk in dit ontwerp.

Section 8

Protection des données

Art. 29

Suite à l'avis du Comité P du 16 juillet 2023, l'article 44/11/3*quinquies*/2, de la loi sur la fonction de police est ici transféré. L'article 29 détermine par qui et comment le contrôle sur les banques de données communes est effectué. Il s'agit *de facto* d'un maintien du dispositif précédent. Une actualisation a toutefois été effectuée et la terminologie utilisée a été adaptée en fonction de la définition des autorités de contrôle.

Art. 30

L'article 30 reprend le contenu de l'article 16 de l'arrêté royal "TF" et de l'arrêté royal "PH" et vise dès lors la responsabilité de la qualité des données à caractère personnel et des informations enregistrées dans la banque de données commune T.E.R. Le dispositif existant actuellement dans l'arrêté royal est maintenu.

Etant donné que sont mises en commun des données et informations enregistrées dans les banques de données des services qui alimentent la banque de données commune T.E.R., par application de leur droit d'écriture, il s'agit aussi d'établir les responsabilités en matière de protection des données et de sécurité.

En matière de qualité des données, il convient de distinguer la responsabilité du responsable du traitement du service qui transmet une donnée à la banque de données commune T.E.R. et celle du responsable du traitement de la banque de données commune T.E.R. même. Dans son avis n° 97/2023 du 16 juin 2023, l'Autorité de protection des données estime qu'il y a lieu de déterminer, dans le projet, qui sont les responsables du traitement, en fonction des différents traitements susceptibles d'être réalisés et non en fonction de la banque de données (§ 109). Comme déjà précisé, la qualité des données relève de la responsabilité propre de chaque service. En fonction du traitement réalisé, il faudra déterminer qui était le responsable du traitement à ce moment précis. Par ailleurs, un ensemble de traitement peut être appelé une banque de données, cela n'est pas interdit.

Ainsi, le responsable du traitement du service fournisseur garde sa responsabilité quant à la licéité de sa

Afdeling 8

Gegevensbescherming

Art. 29

Ingevolge het advies van 16 juli 2023 van Comité P wordt artikel 44/11/3*quinquies*/2 van de wet op het politieambt hier overgebracht. Artikel 29 bepaalt door wie en hoe het toezicht op de gemeenschappelijke gegevensbank wordt uitgevoerd. Het betreft *de facto* een behoud van de vorige bepaling. Niettemin werden er zaken geactualiseerd en werd de gehanteerde terminologie aangepast aan de definitie van de toezichthoudende overheden.

Art. 30

Artikel 30 herneemt de inhoud van artikel 16 van het koninklijk besluit "TF" en van het koninklijk besluit "HP" en beoogt derhalve de verantwoordelijkheid voor de kwaliteit van de persoonsgegevens en de informatie die in de gemeenschappelijke gegevensbank T.E.R. worden opgenomen. De bestaande huidige bepaling in het koninklijk besluit wordt behouden.

Gelet op het feit dat de geregistreerde gegevens en informatie in de gegevensbanken van de diensten die de gemeenschappelijke gegevensbank T.E.R. voeden, met toepassing van hun schrijfrecht, gemeenschappelijk ter beschikking worden gesteld, gaat het er tevens om de verantwoordelijkheden op het vlak van de gegevensbescherming en de beveiliging te bepalen.

Op het vlak van de kwaliteit van de gegevens, moet de verantwoordelijkheid van de verwerkingsverantwoordelijke van de dienst die een gegeven aan de gemeenschappelijke gegevensbank T.E.R. doorzendt, onderscheiden worden van die van de verwerkingsverantwoordelijke van de gemeenschappelijke gegevensbank T.E.R. zelf. In advies nr. 97/2023 van 16 juni 2023 is de Gegevensbeschermingsautoriteit van mening dat het noodzakelijk is om in het ontwerp te bepalen wie de verantwoordelijken voor de gegevensverwerking zijn, op basis van de verschillende verwerkingen die waarschijnlijk zullen worden uitgevoerd en niet op basis van de gegevensbank (§ 109). Zoals reeds verduidelijkt, is elke dienst zelf verantwoordelijk voor de kwaliteit van de gegevens. Naargelang de uitgevoerde verwerking moet worden bepaald wie op dat precieze tijdstip de verwerkingsverantwoordelijke was. Voorts kan een verzameling verwerkingen een gegevensbank worden genoemd; dat is niet verboden.

Zo zal de verwerkingsverantwoordelijke van de aanleverende dienst zijn verantwoordelijkheid behouden over

au bon fonctionnement technique et fonctionnel de sa banque de données afin, par exemple, de s'assurer qu'une donnée transmise ne soit pas altérée par un dysfonctionnement technique.

Le responsable de la banque de données commune T.E.R. s'assure également de l'intégrité, la disponibilité et la confidentialité des données et informations qui y sont enregistrées.

Suite à l'avis du Conseil d'État 73.442/2 du 7 juin 2023, il convient de préciser la nouvelle habilitation du Roi visant à déterminer d'autres règles de responsabilité en matière de protection des données à caractère personnel des services de base et des services partenaires traitant ces données. Il s'agira de prévoir ce qui suit: un premier contrôle de qualité est opéré au sein même du service qui transmet une donnée ou une information à la banque de données commune T.E.R. Les services disposant d'un droit de lecture et d'écriture dans la banque de données commune doivent mettre en place un système de validation interne de leurs propres données afin d'avoir des données adéquates, pertinentes et non excessives au regard des missions et des finalités de la banque de données commune. Un service partenaire peut ajouter des données à propos d'une entité déjà enregistrée sans modifier/supprimer celles qui existent déjà. Seul le service qui a enregistré une donnée peut la modifier, la rectifier et la supprimer. Si un autre service estime qu'une donnée doit être modifiée, rectifiée ou supprimée, il en informe le service qui l'a enregistrée en vue de procéder le cas échéant aux adaptations nécessaires. En cas de désaccord, le responsable opérationnel prend la décision finale.

Dans le cadre de cet article, on peut également rappeler que dans son avis du 20 juin 2023, le COC recommande à la GPI de travailler avec ce qui se fait pratiquement déjà sur le terrain par ceux qui peuvent être assimilés à des responsables opérationnels et qui assurent l'alimentation de la banque de données commune T.E.R. et qui sont les mieux placés pour garantir la qualité des données à caractère personnel et des informations.

verwerkingsverantwoordelijke van de gemeenschappelijke gegevensbank T.E.R. dient te waken over de goede technische en functionele werking van zijn gegevensbank, teneinde bijvoorbeeld om ervoor te zorgen dat een doorgezonden gegeven niet gewijzigd wordt door een technische storing.

De verwerkingsverantwoordelijke van de gemeenschappelijke gegevensbank T.E.R. waakt eveneens over de integriteit, de beschikbaarheid en de vertrouwelijkheid van de gegevens en informatie die er in geregistreerd zijn.

Ingevolge advies nr. 73.442/2 van 7 juni 2023 van de Raad van State moet een verduidelijking worden gegeven van de nieuwe machtiging van de Koning om andere regels te bepalen inzake de verantwoordelijkheid op het gebied van de bescherming van persoonsgegevens van de basisdiensten en de partnerdiensten die deze gegevens verwerken. Dat houdt het volgende in: er wordt een eerste kwaliteitscontrole uitgevoerd binnen de dienst zelf die informatie of een gegeven doorzendt naar de gemeenschappelijke gegevensbank T.E.R. De diensten met een lees- en schrijfrecht in de gemeenschappelijke gegevensbank moeten een intern validatiesysteem voor hun eigen gegevens opzetten teneinde te beschikken over gegevens die toereikend, ter zake dienend en niet bovenmatig zijn in verhouding tot de opdrachten en de doeleinden van de gemeenschappelijke gegevensbank. Een partnerdienst kan gegevens over een reeds opgenomen entiteit toevoegen zonder de reeds bestaande gegevens te wijzigen/verwijderen. Enkel de dienst die een gegeven heeft opgenomen, kan het wijzigen, verbeteren en verwijderen. Als een andere dienst van mening is dat een gegeven moet worden gewijzigd, verbeterd of verwijderd, stelt hij de dienst die het heeft opgenomen daarvan in kennis om in voorkomend geval over te gaan tot de nodige aanpassingen. In geval van onenigheid neemt de operationeel verantwoordelijke de eindbeslissing.

In het kader van dit artikel moet er ook worden gewezen dat het COC in het advies van 20 juni 2023 aanbeveelt dat de GPI werkt met zogenoemde "operationeel verantwoordelijken" (wat in de praktijk in het veld reeds gebeurt), die instaan voor de voeding van de gemeenschappelijke gegevensbank T.E.R. en derhalve ook het best geplaatst zijn om in te staan voor de kwaliteit van de persoonsgegevens en informatie.

CHAPITRE 3

Enrichissement des données relatives aux entités et suivi d'une entité validée dans la banque de données commune

Ce chapitre concerne les conséquences de l'enregistrement d'une entité dans la banque de données commune T.E.R.

Du 17 mai au 20 juin 2021 a lieu l'affaire Conings. Ce dernier fut traqué à la suite de ses menaces contre des personnalités politiques belges et contre un virologue connu et fut finalement retrouvé mort. Il était enregistré dans la banque de données commune "TF" pour extrémisme de droite avec un niveau de menace évalué à 3. Lors de sa traque, ce militaire avait emporté des armes et des munitions de la caserne où il officiait en utilisant les accès dont il disposait toujours malgré son inscription dans la banque de données commune "TF" et le retrait de son habilitation de sécurité.

Cette affaire a permis de réaffirmer l'importance de l'échange de données et d'informations entre les différents services compétents en matière de terrorisme-extrémisme et la nécessité d'une communication optimale entre eux en vue de la prise de mesures appropriées le plus rapidement possible. Par rapport à ce qu'indique l'Autorité de protection des données dans son avis n° 97/2023 du 16 juin 2023 (§§ 84 à 92), il faut préciser que l'affaire Conings n'est pas utilisée pour justifier l'accroissement de l'ingérence résultant de l'inclusion d'acteurs ne relevant pas de la chaîne pénale et de sécurité dans les autorités tenues de communiquer et de se voir communiquer des données, relatives aux entités, dans le cadre des concertations en TFL. Cette affaire est citée à titre illustratif car elle démontre qu'il y a eu un manquement à moment donné et qu'il est dès lors nécessaire de rester attentif à la problématique. Le but premier du projet est bien de répondre aux recommandations de la Commission d'enquête parlementaire sur les attentats de 2016. Par ailleurs, la présence de l'office des étrangers aux concertations en TFL se justifie dans la mesure où statistiquement, la majorité des entités sont de nationalité étrangère (cf. *infra*).

Afin de favoriser et optimiser davantage cet échange et cette communication, le législateur prévoit désormais, dans le chapitre 3, d'une part, que l'échange de données et informations au sujet d'une entité se fait au sein d'une plateforme de concertation nommée "la TFL" et d'autre part, que la TFL, se concerte, dès la validation d'une

HOOFDSTUK 3

Verrijking van gegevens over entiteiten en opvolging van een in de gemeenschappelijke gegevensbank gevalideerde entiteit

Dit hoofdstuk heeft betrekking op de gevolgen van de opname van een entiteit in de gemeenschappelijke gegevensbank T.E.R.

Van 17 mei tot en met 20 juni 2021 vond de zaak Conings plaats. Op die laatste werd een klopjacht gehouden naar aanleiding van zijn bedreigingen tegen Belgische politieke persoonlijkheden en tegen een bekende viroloog. Hij werd uiteindelijk dood teruggevonden. Hij was opgenomen in de gemeenschappelijke gegevensbank "TF" wegens rechts-extremisme met een dreigingsniveau 3. Tijdens de klopjacht had die militair wapens en munitie meegenomen uit de kazerne waar hij werkzaam was door gebruik te maken van de toegang waarover hij nog steeds beschikte ondanks zijn inschrijving in de gemeenschappelijke gegevensbank "TF" en de intrekking van zijn veiligheidsmachtiging.

Deze zaak heeft opnieuw het belang van de uitwisseling van gegevens en van informatie tussen de verschillende diensten die bevoegd zijn op het gebied van terrorisme-extrémisme en de noodzaak van een optimale communicatie tussen hen teneinde zo snel mogelijk gepaste maatregelen te kunnen nemen, bevestigd. Met betrekking tot wat de Gegevensbeschermingsautoriteit in advies nr. 97/2023 van 16 juni 2023 (§§ 84 tot 92) aangeeft, moet er worden verduidelijkt dat de zaak-Conings niet wordt aangegrepen ter rechtvaardiging van de grotere inmenging ten gevolge van de integratie van actoren buiten de straf- en veiligheidsketen bij de overheden die gegevens met betrekking tot entiteiten in het kader van LTF-overleg moeten meedelen en meegedeeld moeten krijgen. Die zaak is ter illustratie aangehaald, aangezien hij aantoont dat er op een bepaald moment een tekortkoming was en dat er daarom aandacht moet blijven worden geschonken aan de problematiek. Het ontwerp heeft als primair doel om tegemoet te komen aan de aanbevelingen van de parlementaire onderzoekscommissie rond de aanslagen van 2016. Voorts is de aanwezigheid van de Dienst Vreemdelingenzaken bij LTF-overleg gerechtvaardigd doordat de meeste entiteiten statistisch gezien een vreemde nationaliteit hebben (zie *infra*).

Teneinde die uitwisseling en die communicatie meer te optimaliseren en te bevorderen, voorziet de wetgever voortaan, in hoofdstuk 3, enerzijds erin dat de uitwisseling van gegevens en informatie inzake een entiteit gebeurt in een overlegplatform, "de LTF" genaamd, en anderzijds dat de LTF, vanaf de validatie van een

entité dans la banque de données commune T.E.R. au sujet d'éventuelles mesures qui peuvent être prises suite à l'enregistrement d'une entité dans la banque de données commune T.E.R. Le résultat de cette concertation est transmis à l'autorité compétente pour décider de la mesure en question.

Dans son avis 97/2023 du 16 juin 2023, l'Autorité de protection des données indique qu'il est "nécessaire que les "éléments essentiels" des traitements relatifs aux données enregistrées dans la BDC ET aux données communiquées à l'occasion des concertations en TFL soient définis dans une norme de rang législatif." (§ 18). Toutefois, on se trouve ici dans le cadre d'une concertation. La majorité des traitements qui ont lieu dans le cadre de cette concertation sont ceux de la banque de données commune T.E.R. Par conséquent, ce sont les règles de la banque de données commune T.E.R. définies par le présent projet qui s'appliquent. Dans le cadre des entités qui ne sont pas encore enregistrées dans la banque de données commune T.E.R., les données traitées sont celles des services qui sont en leur possession et les traitements se font sous leur responsabilité. Ainsi par exemple, le président de la TFL, à savoir le directeur coordinateur administratif de la police fédérale, lorsqu'il prépare sa réunion doit gérer les données qu'il va traiter durant cette préparation selon les règles de la loi sur la fonction de police. Il en va de même pour les autres organisations qui devront respecter leurs propres législations.

En outre, l'Autorité fait des observations concernant les CSIL-R (§§ 61 à 63). À ce sujet, il faut préciser que l'Autorité a une bonne lecture du projet dans la mesure où le dispositif en projet ne concerne pas les CSIL-R. Ces dernières relèvent de la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et travaillent au niveau de la prévention sociale.

Art. 31

En vue d'enrichir les données à caractère personnel et informations relatives à l'ensemble des entités, c'est-à-dire de les compléter, les développer ou encore les étoffer, et d'assurer le suivi et la prise de mesure à l'égard de celles qui ont été validées dans la banque de données commune T.E.R., l'échange de données ou d'informations ainsi que la concertation entre tous les services impliqués dans la lutte contre l'extrémisme et le terrorisme sont primordiales. Pour répondre à l'Autorité de protection des données (§§ 43 et 44 de l'avis 97/2023 du 16 juin 2023), on peut préciser que l'enrichissement des données et informations relative à une entité

entiteit in de gemeenschappelijke gegevensbank T.E.R., overleg pleegt over eventuele maatregelen die kunnen worden genomen na de opname van een entiteit in de gemeenschappelijke gegevensbank T.E.R. Het resultaat van dit overleg wordt overgezonden aan de bevoegde overheid om te beslissen over de betrokken maatregel.

In advies nr. 97/2023 van 16 juni 2023 wijst de Gegevensbeschermingsautoriteit op de noodzaak dat "de "essentiële elementen" van de verwerkingen met betrekking tot de in de GGB opgeslagen gegevens EN de tijdens het LTF-overleg meegedeelde gegevens in een norm van wetgevende rang worden omschreven." (§ 18). Hier gaat het echter om overleg. De meeste verwerkingen die in het kader van dat overleg plaatsvinden, zijn die van de gemeenschappelijke gegevensbank T.E.R. Bijgevolg zijn de bij dit ontwerp vastgelegde regels van de gemeenschappelijke gegevensbank T.E.R. van toepassing. De gegevens van de entiteiten die nog niet in de gemeenschappelijke gegevensbank T.E.R. zijn opgenomen, worden verwerkt onder de verantwoordelijkheid van de diensten die ze ter beschikking hebben. Aldus moet bijvoorbeeld de voorzitter van de LTF, dus de bestuurlijke directeur-coördinator van de federale politie, bij het voorbereiden van zijn vergadering de gegevens beheren die hij tijdens zijn voorbereiding zal verwerken volgens de regels van de wet op het politieambt. Hetzelfde geldt voor de andere organisaties die hun eigen wetgeving zullen moeten naleven.

Voorts formuleert de Gegevensbeschermingsautoriteit opmerkingen rond de LIVC-R's (§§ 61 tot 63). In dat verband moet worden verduidelijkt dat er een goede lezing is vanwege de Gegevensbeschermingsautoriteit met betrekking tot het ontwerp, aangezien de ontworpen bepaling geen betrekking heeft op de LIVC-R's. Die vallen onder de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en zijn werkzaam op het gebied van maatschappelijke preventie.

Art. 31

Met het oog op de verrijking van persoonsgegevens en informatie over alle entiteiten, met andere woorden het aanvullen, uitwerken en uitbreiden ervan, en de verzekering van de opvolging en het nemen van maatregelen ten aanzien van de entiteiten die in de gemeenschappelijke gegevensbank T.E.R. zijn gevalideerd, zijn de uitwisseling van gegevens of van informatie alsmede het overleg tussen alle diensten die betrokken zijn bij de strijd tegen extremisme en terrorisme van cruciaal belang. In antwoord op de Gegevensbeschermingsautoriteit (§§ 43 en 44 van advies nr. 97/2023 van 16 juni 2023) kan worden gepreciseerd dat de verrijking van gegevens

a notamment pour but d'une part, de contextualiser des données la concernant et d'autre part, de mettre à jour des données et des informations déjà enregistrées dans la banque de données commune T.E.R. et/ou d'apporter des nouveaux éléments. La contextualisation des données et informations est importante dans la mesure où la banque de données commune T.E.R. ne contient pas toutes les informations disponibles des services de base ou des services partenaires sur les entités (la banque de données commune T.E.R. ne reprend pas, par exemple, le contenu *in extenso* des procès-verbaux). Elle permet donc de donner tout le contexte relatif à la donnée enregistrée dans la banque de données commune T.E.R. (personne, véhicule, ...). Par ailleurs, lors de la TFL, et de la discussion avec les différents services présents, il peut ressortir qu'il y ait des nouvelles données ou informations à enregistrer dans la banque de données commune T.E.R. et qu'il faille donc l'"enrichir" ou qu'il soit nécessaire de mettre des données ou de l'information déjà enregistrées à jour. Ainsi, les données sont échangées en vue de leur enregistrement. Enfin, il faut rappeler que le RGPD ne s'applique pas à des réunions. Son application nécessite qu'il y ait un support. Par ailleurs, le projet est conçu en termes de banque de données commune et non pas en termes de traitements et une banque de données commune est un ensemble de traitement. Enfin, au sujet de cet article, il nous semble que l'Autorité de protection des données (§ 92) traite de questions opérationnelles qui ne relèvent pas de sa compétence, d'autant plus qu'un échange ne constitue pas un traitement. L'objectif de la plateforme (TFL) est d'avoir une mise en commun d'informations et d'en discuter. Ensuite, chaque service, sur base de ses propres règles, prend les mesures qu'il estime nécessaire.

L'article 31 prévoit que l'échange de données concernant une entité enregistrée dans la banque de données commune s'effectue au sein de plateformes nommées "Taskforces locales" (TFL). Alors que les cellules de Sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme (CSIL-R), créées par la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme, travaillent au niveau de la prévention sociale, les TFL constituent un réseau permanent établi dans une optique sécuritaire.

Au sein de la TFL, sont échangées non seulement les données à caractère personnel et les informations non classifiées contenues dans la banque de données commune T.E.R. mais également d'autres données à caractère personnel ou informations considérées comme pertinentes, y compris les classifiées et celles qui proviennent de services qui ne sont pas tenus d'alimenter la banque de données commune T.E.R. Il ne serait en

en van informatie betreffende een entiteit met name als doel heeft om de op hem toepasselijke gegevens te contextualiseren en om reeds in de gemeenschappelijke gegevensbank T.E.R. opgenomen gegevens en informatie bij te werken en/of er nieuwe elementen aan toe te voegen. De contextualisering van de gegevens en van de informatie is belangrijk omdat de gemeenschappelijke gegevensbank T.E.R. niet alle beschikbare informatie van de basisdiensten of de partnerdiensten omtrent de entiteiten bevat (in de gemeenschappelijke gegevensbank T.E.R. wordt de inhoud van processen-verbaal bijvoorbeeld niet *in extenso* overgenomen). Op die manier kan het in de gemeenschappelijke gegevensbank opgenomen gegeven dus volledig in zijn context worden geplaatst (persoon, voertuig enz.). Tijdens de LTF en de bespreking met de verschillende aanwezige diensten kan bovendien blijken dat er nieuwe gegevens of informatie moeten worden opgenomen in de gemeenschappelijke gegevensbank T.E.R. en dat die dus moet worden "verrijkt" of dat er reeds opgenomen gegevens of informatie moeten worden bijgewerkt. Aldus worden de gegevens uitgewisseld met het oog op de opnemings ervan. Tot slot moet er worden benadrukt dat de AVG niet van toepassing is op vergaderingen. Ze wordt enkel toegepast als er een drager is. Het ontwerp is bovendien gericht op een gemeenschappelijke gegevensbank en niet op verwerkingen, en een gemeenschappelijke gegevensbank is een verzameling verwerkingen. Ons lijkt dat de Gegevensbeschermingsautoriteit met betrekking tot dit artikel operationele kwesties bespreekt die niet tot haar bevoegdheid behoren, te meer omdat een uitwisseling geen verwerking is. Het doel van het platform (LTF) is dat er informatie kan worden gebundeld en besproken. Vervolgens treft elke dienst op basis van zijn eigen regels de maatregelen die hij nodig acht.

Artikel 31 voorziet erin dat de uitwisseling van gegevens met betrekking tot een in de gemeenschappelijke gegevensbank opgenomen entiteit in platformen gebeurt die "lokale taskforces" (LTF) worden genoemd. Terwijl de lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme (LIVC R), opgericht bij de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme, werken op het gebied van sociale preventie, vormen de LTF een permanent netwerk dat vanuit het perspectief van veiligheid is opgericht.

In de LTF worden niet enkel de persoonsgegevens en de niet geclassificeerde informatie vervat in de gemeenschappelijke gegevensbank T.E.R., uitgewisseld, maar ook andere relevante geachte persoonsgegevens of informatie, daaronder begrepen de geclassificeerde en deze die afkomstig zijn van diensten die de gemeenschappelijke gegevensbank T.E.R. niet moeten voeden. Het zou namelijk ondenkbaar zijn dat dit soort informatie

effet pas concevable que pour ce phénomène particulièrement sérieux ce type d'informations ne soient pas échangées loyalement entre les services concernés. Toutefois, tant que ces informations sont classifiées ou confidentielles, elles ne pourront être mentionnées dans le rapportage des task force locales. Maintenant, lorsqu'une donnée ou information classifiée ou confidentielle est intéressante à enregistrer dans la banque de données commune T.E.R., rien n'empêche le service propriétaire de la donnée ou information concernée de réévaluer la nécessité de maintenir la protection et de procéder, le cas échéant, à une déclassification.

Comme souligné par le Conseil d'État dans son avis 73.442/2 du 7 juin 2023, cet article ne peut pas être interprété "comme permettant l'enregistrement dans la banque de données commune T.E.R. de données ou d'informations classifiées, celles-ci pouvant tout au plus faire l'objet d'échanges lors des réunions de la Task force locale."

Les services sont tenus de n'échanger que les données à caractère personnel et les informations qu'ils ont le droit de traiter dans le cadre de leurs missions.

Il va de soi que les services de police judiciaires, en ce qui concerne l'échange des informations judiciaires dans le cadre de la TFL, seront tenus de respecter les directives du Collège des procureurs généraux à ce sujet (actuellement il s'agit de la circulaire confidentielle COL 18/2020 du Collège des procureurs généraux près les cours d'appel relative à l'approche judiciaire en matière des *foreign terrorist fighters*, des *Homegrown Terrorist Fighters*, des *Propagandistes de haine*, des *extrémistes potentiellement violents* et des *personnes condamnées pour terrorisme*) et que l'échange de données au sein de la TFL ne peut compromettre l'exercice de l'action publique ou la sécurité des personnes.

Comme précisé ci-avant, pour garantir le bon fonctionnement des TFL, il s'est avéré nécessaire de pouvoir partager des informations confidentielles, également par les membres des TFL qui sont tenus par le secret professionnel. L'article 458ter du Code pénal prévoit une exception à la pénalisation de la violation du secret professionnel, réglée à l'article 458 et suivants du Code pénal, pour certaines structures de concertation. L'article 31 du présent avant-projet de loi soumet la TFL au champ d'application de l'article 458ter du Code pénal. Ce principe est important pour les participants qui sont tenus au secret professionnel dans le chef de leur fonction, mais aussi pour ceux qui n'y sont pas tenus. En effet, l'article 458ter, § 2, stipule que les participants sont tenus au secret pour ce qui concerne les secrets communiqués durant la concertation.

over dit bijzonder ernstig fenomeen niet op loyale wijze uitgewisseld zou worden tussen de betrokken diensten. Zolang deze informatie echter geclassificeerd of vertrouwelijk is, zal ze niet in de verslaggeving van de lokale task forces kunnen vermeld worden. Wanneer een geclassificeerd of vertrouwelijke gegeven of informatie interessant is om te registreren in de gemeenschappelijke gegevensbank T.E.R., verhindert niets de dienst die eigenaar is van het gegeven of de informatie in kwestie de nood aan bescherming opnieuw te evalueren en in voorkomend geval over te gaan tot een declassificatie.

Zoals de Raad van State aanhaalt in advies nr. 73.442/2 van 7 juni 2023, mag dit artikel "niet aldus worden geïnterpreteerd dat geclassificeerde gegevens of geclassificeerde informatie in de gemeenschappelijke gegevensbank T.E.R. kunnen worden geregistreerd. Die gegevens en informatie mogen hoogstens tijdens vergaderingen van de lokale taskforce worden uitgewisseld."

De diensten zijn ertoe gehouden enkel de persoonsgegevens en de informatie uit te wisselen waarvoor zij het recht hebben ze te verwerken in het kader van hun opdrachten.

Het spreekt vanzelf dat, wat de gerechtelijke informatie-uitwisseling in het kader van de LTF betreft, de gerechtelijke politiediensten zich zullen moeten houden aan de richtlijnen van het College van procureurs-generaal hierover (op dit ogenblik is dit de vertrouwelijke omzendbrief COL 18/2020 van het College van procureurs-generaal bij de hoven van beroep betreffende de gerechtelijke aanpak inzake de *Foreign terrorist fighters*, de *Homegrown terrorist fighters*, de *Haatpropagandisten*, de *potentieel gewelddadige extremisten* en de *terrorismeveroordeelden*), en dat de uitwisseling van gegevens binnen de TFL de uitoefening van de strafvordering en de veiligheid van personen niet in het gedrang mag brengen.

Zoals hierboven vermeld, om de goede werking van de LTF's te waarborgen is het noodzakelijk gebleken dat er vertrouwelijke informatie kan gedeeld worden, ook door deelnemers van de LTF die gebonden zijn door het beroepsgeheim. Artikel 458ter van het Strafwetboek voorziet een uitzondering op de strafbaarheidstelling van de schending van het beroepsgeheim, geregeld in artikel 458 en volgende van het Strafwetboek, voor bepaalde overlegstructuren. Artikel 31 van voorliggend voorontwerp brengt de LTF onder het toepassingsgebied van 458ter van het Strafwetboek. Dit is van belang voor de deelnemers die gebonden zijn aan het beroepsgeheim uit hoofde van hun functie, maar ook voor diegenen die hierdoor niet gebonden zijn. Artikel 458ter, § 2, stelt immers dat de deelnemers tot geheimhouding verplicht zijn wat betreft de tijdens het overleg meegedeelde geheimen.

Pour qu'une TFL puisse être considérée comme structure de concertation conformément à l'article 458ter du Code pénal, elle doit satisfaire à certaines conditions. La concertation doit tout d'abord être organisée soit par ou en vertu d'une loi, d'un décret ou d'une ordonnance, soit moyennant une autorisation motivée du procureur du Roi. Il convient de déterminer au moins qui peut participer à la concertation, avec quelle finalité et selon quelles modalités la concertation aura lieu. Le présent avant-projet de loi satisfait à cette exigence.

L'article 458ter du Code pénal stipule en outre que la concertation "peut exclusivement être organisée soit en vue de protéger l'intégrité physique et psychique de la personne ou de tiers, soit en vue de prévenir les délits visés au Titre I^{ter} du Livre II ou les délits commis dans le cadre d'une organisation criminelle, telle qu'elle est définie à l'article 324bis."

Les TFL satisfont également à cette exigence étant donné qu'elles ont notamment pour but d'enrichir les données à caractère personnel et informations relatives à l'ensemble des entités enregistrées dans la banque de données commune T.E.R. dont la finalité est "le traitement commun, par tout ou partie des services de base et des services partenaires, des données à caractère personnel et des informations relatives aux missions de prévention et de suivi du terrorisme et de l'extrémisme, lorsqu'il peut mener au terrorisme, au sens de l'article 8, 1^o, b) et c) de la loi du 30 novembre 1998 des services de renseignement et de sécurité, de ces services, chacun dans le cadre de ses compétences légales" (art. 3 en projet).

Art. 32

Cet article prévoit que la TFL, présidée par le directeur coordinateur administratif de la police fédérale ou son représentant, constitue la plateforme au sein de laquelle se concertent les services de renseignements et de sécurité, l'Organe de coordination pour l'analyse de la menace, la police fédérale et la police locale, l'Office des étrangers ainsi que le Ministère public. La remarque formulée par le Conseil d'État dans son avis 77.443/2 du 7 juin 2023 au sujet de l'absence d'indication quant au nombre de membres par catégories et quant aux modalités de fonctionnement de la TFL n'a pas été suivie. Après réexamen, il faut préciser que les modalités liées au fonctionnement de la TFL tel que le nombre de réunion ou encore le nombre de participants sont réglées par la circulaire ministérielle du 22 mai 2018 relative à l'échange d'informations et

Opdat een TFL kan beschouwd worden als een overlegstructuur overeenkomstig artikel 458ter van het Strafwetboek, dient deze te voldoen aan een aantal voorwaarden. Ten eerste moet het overleg worden georganiseerd hetzij bij of krachtens een wet, decreet of ordonnantie, hetzij bij een met redenen omklede toestemming van de procureur des Konings. Bovendien dient deze ten minste te bepalen wie aan het overleg kan deelnemen, met welke finaliteit en volgens welke modaliteiten het overleg zal plaatsvinden.

Artikel 458ter van het Strafwetboek bepaalt daarnaast dat het overleg "uitsluitend worden georganiseerd, hetzij met het oog op de bescherming van de fysieke en psychische integriteit van de persoon of van derden, hetzij ter voorkoming van de misdrijven bedoeld in Titel I^{ter} van Boek II of van de misdrijven gepleegd in het raam van een criminele organisatie, zoals bepaald in artikel 324bis."

De LTF's voldoen ook aan vereiste, aangezien het doel ervan met name de verrijking is van de persoonsgegevens en informatie met betrekking tot alle in de gemeenschappelijke gegevensbank T.E.R. opgenomen entiteiten met als doeleinde "de gemeenschappelijke verwerking [...] door alle of een deel van de basisdiensten en de partnerdiensten, van de persoonsgegevens en informatie betreffende de opdrachten inzake de voorkoming en de opvolging van terrorisme en extremisme, dat kan leiden tot terrorisme, in de zin van artikel 8, 1^o, b) en c), van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, van die diensten, elk in het kader van zijn wettelijke bevoegdheden" (ontworpen artikel 3).

Art. 32

Dit artikel voorziet erin dat de LTF, voorgezeten door de bestuurlijke directeur-coördinator van de federale politie of zijn vertegenwoordiger, het platform vormt waarin de inlichtingen- en veiligheidsdiensten, het Coördinatieorgaan voor de dreigingsanalyse, de federale politie en de lokale politie, de Dienst Vreemdelingenzaken en het openbaar ministerie overleg plegen. De opmerking van de Raad van State in advies nr. 77.443/2 van 7 juni 2023 over het feit dat er niets is bepaald in verband met het aantal leden per categorie, noch in verband met de nadere regels voor de werkwijze van de LTF, werd niet gevolgd. Na heroverweging moet er worden verduidelijkt dat de nadere regels in verband met de werking van de LTF, zoals het aantal vergaderingen en het aantal deelnemers, worden geregeld bij de ministeriële

au suivi des *terrorist fighters* et des propagandistes de haine. Cette circulaire devra être mise à jour.

Dans son avis n° 97/2023 du 16 juin 2023, l'Autorité de protection des données s'interroge sur l'absence d'alignement entre services de base/partenaires de la banque de données commune et participants de droit ou invités aux coordinations dans le cadre des TFL (§ 110). Comme précisé précédemment, la TFL est un réseau permanent établi dans une optique sécuritaire, raison pour laquelle les services de renseignements et de sécurité, l'OCAM, la police fédérale et locale ainsi que le Ministère public y participent. La présence permanente de la Direction générale de l'Office des étrangers du Service public fédéral Intérieur se justifie également dans la mesure où statistiquement, la majorité des entités sont de nationalité étrangère. La TFL peut toutefois inviter d'autres intervenants si leur input est nécessaire (cf. *infra*). Par ailleurs, il faut rappeler que Les CSIL-R et les TFL se complètent. Alors que la TFL vise un suivi réactif et répressif dans une optique de sécurité, la CSIL-R est axée sur la prévention et le suivi. Il est donc possible qu'une entité soit suivie à deux "niveaux".

En outre, chaque zone de police désigne au moins un membre de la Police locale en tant qu'Information Officer. L'Information Officer participe à la TFL et fait le lien entre la TFL et la CSIL-R visée dans la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme en vue d'une collaboration efficace entre la TFL et la CSIL-R.

Sur ce point, le Comité R s'interroge sur le cas d'une entité active sur le territoire de plusieurs arrondissements judiciaires et donc TFL (§ 42). En principe, la TFL compétente pour traiter d'une entité est désignée sur base du dernier domicile connu de la personne concernée. Si l'entité est une personne morale qui a des unités d'établissements dans plusieurs arrondissements judiciaires par exemple, il s'agira de prendre en compte la dernière adresse du siège social.

Étant donné le caractère sensible des données et informations échangées au sein de la TFL, l'article 32 prévoit que le président et ses membres disposent d'une habilitation de sécurité au moins du niveau "secret" en vertu de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

omzendbrief van 22 mei 2018 betreffende de informatie-uitwisseling rond en de opvolging van *Terrorist Fighters* en Haatpropagandisten. Die omzendbrief zal moeten worden bijgewerkt.

In advies nr. 97/2023 van 16 juni 2023 heeft de Gegevensbeschermingsautoriteit vragen bij het gebrek aan afstemming tussen de basis-/partnerdiensten van de gemeenschappelijke gegevensbank en ambtshalve of uitgenodigde deelnemers aan de coördinatie van LTF's (§ 110). Zoals eerder toegelicht is de LTF een permanent netwerk dat vanuit het perspectief van veiligheid is opgericht, vandaar de betrokkenheid van de veiligheids- en inlichtingendiensten, het OCAD, de federale en lokale politie en het openbaar ministerie. Dat de Algemene Directie Dienst Vreemdelingenzaken van de Federale Overheidsdienst Binnenlandse Zaken vast aanwezig is, is tevens gerechtvaardigd doordat de meeste entiteiten statistisch gezien een vreemde nationaliteit hebben. De LTF kan echter anderen uitnodigen indien hun input nodig is (zie *infra*). Bovendien zij erop gewezen dat de LVC-R's en de LTF's elkaar aanvullen. Het doel van de LTF is om snel en krachtadig op te treden vanuit veiligheidsoogpunt, terwijl de LVC-R gericht is op preventie en opvolging. Het kan dus zijn dat een entiteit op twee "niveaus" wordt opgevolgd.

Bovendien wijst elke politiezone ten minste een lid van de lokale politie als Information Officer aan. De Information Officer neemt deel aan de LTF en vormt de brug tussen de LTF en de LVC R bedoeld in de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme met het oog op een doeltreffende samenwerking tussen de LTF en de LVC R.

In dat verband vraagt Comité I zich af wat er moet gebeuren met een entiteit die actief is op het grondgebied van verschillende gerechtelijke arrondissementen en dus LTF's. In principe wordt de LTF die bevoegd is voor de behandeling van een entiteit, aangewezen op basis van de laatst bekende woonplaats van de betrokkene. Is de entiteit bijvoorbeeld een rechtspersoon met vestigingseenheden in verschillende gerechtelijke arrondissementen, moet er rekening worden gehouden met het laatste adres van de maatschappelijke zetel.

Gelet op de gevoelige aard van de gegevens en informatie die in de LTF worden uitgewisseld, voorziet artikel 32 dat de voorzitter en de leden ervan over een veiligheidsmachtiging beschikken van ten minste het niveau "geheim" krachtens de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

Pour rappel, les magistrats du Ministère public n'ont pas besoin d'habilitation de sécurité (cf. article 8 de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité). Les autres membres du ministère public (par exemple, les juristes ou le personnel administratif), en revanche, doivent être titulaires d'une habilitation de sécurité de niveau "secret". Le Collège des procureurs généraux désignera, dans une circulaire, les catégories de personnes au sein du ministère public qui doivent avoir accès à la banque de données commune T.E.R., à condition qu'elles soient titulaires de l'habilitation de sécurité susmentionnée.

Afin que la TFL puisse travailler de manière optimale et lorsque cela s'avère nécessaire pour le suivi ciblé d'une entité, le président peut inviter d'autres services, organes ou instances en raison de leurs compétences ou fonctions à participer à la TFL et ce, le temps strictement nécessaire à la contribution qu'ils peuvent apporter à la TFL. Ces services, organes ou instances sont invitées pour fournir des données, éclairer un point précis de leur expertise. Ainsi, comme précisé par le Conseil d'État dans son avis 73.442/2 du 7 juin 2023, et en réponse aux remarques de l'Autorité de protection des données dans son avis 97/2023 du 16 juin 2023 (§§ 45-46 et 91) et du Comité R dans son avis du 13 juillet 2023 (§ 31), "l'article 32, § 1^{er}, alinéa 4, en projet doit être interprété comme permettant aux "autres services, organes ou instances" invités à participer aux réunions de la Task force locale de communiquer des données ou des informations dont ils seraient détenteurs en raison de leur mission en vue d'enrichir les données ou informations contenues dans la banque de données. Ils ne pourraient en revanche se voir communiquer des données ou informations dont les autres membres de la Task force locale seraient détenteurs.". Très concrètement, un expert sera présent uniquement durant "son point" et quittera ensuite la réunion après son exposé. En outre, une concertation entre le président et les participants à la TFL permettra de n'inviter que des services, organes ou instances fiables. La concertation devrait aussi évaluer si lors de l'échange, il est nécessaire de communiquer des informations sensibles ou classifiées auquel cas une habilitation sera nécessaire. À noter que pour les services partenaires visés à l'article 2, 3°, 1), une habilitation de sécurité sera toujours nécessaire. Dans son avis du 13 juillet 2023, le Comité R demande de mieux définir quelles catégories de "services, organes ou instances" peuvent être invités à une T.F.L. (§ 31). Comme cela est indiqué dans le dispositif, il s'agit d'inviter ceux qui peuvent apporter leur expertise dans le cadre du suivi d'une entité déterminée. Le but est d'être le plus large possible. Le critère déterminant est l'apport

Ter herinnering, de magistraten van het Openbaar Ministerie hebben geen veiligheidsmachtiging nodig (cfr. artikel 8 van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen). De andere leden van het Openbaar Ministerie (bv juristen of administratief personeel) moeten daarentegen wel houder zijn van een veiligheidsmachtiging van het niveau "geheim". Het College van procureurs-generaal zal in een omzendbrief de categorieën van personen binnen het Openbaar Ministerie aanduiden die toegang nodig hebben tot de gemeenschappelijke gegevensbank T.E.R., op voorwaarde dat deze beschikken over voormelde veiligheidsmachtiging.

Om ervoor te zorgen dat de LTF optimaal kan werken en wanneer zulks nodig blijkt voor de gerichte opvolging van een entiteit, kan de voorzitter andere diensten, organen of instanties op de LTF uitnodigen wegens hun bevoegdheden of functies, en zulks zolang strikt noodzakelijk is voor de bijdrage die ze de LTF kunnen leveren. Die diensten, organen of instanties worden uitgenodigd om gegevens te verstrekken, een welbepaald aspect van hun deskundigheid toe te lichten. Zoals verduidelijkt door de Raad van State in advies nr. 73.442/2 van 7 juni 2023 en in antwoord op de opmerkingen van de Gegevensbeschermingsautoriteit in advies nr. 97/2023 van 16 juni 2023 (§§ 45-46 et 91) en van Comité I in het advies van 13 juli 2023 (§ 31), moet "het ontworpen artikel 32, § 1, vierde lid, zo [...] worden geïnterpreteerd dat "andere diensten, organen of instanties" die zijn uitgenodigd om deel te nemen aan de vergaderingen van de lokale taskforce, gegevens of informatie die ze in het kader van hun opdracht bezitten, kunnen meedelen om de gegevens of de informatie die al in de gegevensbank zitten, te verrijken. Ze zouden daarentegen geen gegevens of informatie kunnen ontvangen die de andere leden van de lokale taskforce zouden bezitten.". Concreet is een deskundige louter aanwezig gedurende "zijn punt" en verlaat hij de vergadering na zijn uiteenzetting. Bovendien maakt overleg tussen de voorzitter en de deelnemers aan de LTF maakt het mogelijk om enkel betrouwbare diensten, organen of instanties uit te nodigen. Tijdens dat overleg zou ook moeten worden beoordeeld of bij de uitwisseling gevoelige of geclassificeerde informatie moet worden meegedeeld, in welk geval een machtiging noodzakelijk is. Merk op dat voor de in artikel 2, 3°, 1), bedoelde partnerdiensten altijd een veiligheidsmachtiging vereist is. In het advies van 13 juli 2023 vraagt Comité I om beter te omschrijven welke categorieën van "diensten, organen of autoriteiten" kunnen worden uitgenodigd voor een LTF (§ 31). Zoals het in de bepaling is verwoord, is het de bedoeling diegenen uit te nodigen die hun deskundigheid kunnen inbrengen bij de opvolging van

que peut avoir une personne ou un service pour le cas examiné en T.F.L.

Afin d'uniformiser le fonctionnement de chaque TFL créée, l'article 32 prévoit désormais que la coordination administrative, le secrétariat et le suivi de la TFL sont assurés par le directeur coordinateur administratif de la police fédérale ou les personnes qu'il désigne et, ce, afin de pouvoir déléguer ces tâches. Ainsi, par exemple, lorsqu'il faudra transmettre le résultat de la concertation visée à l'article 32 à l'autorité compétente pour prendre la mesure à l'égard de l'entité, le directeur coordinateur pourra désigner un partenaire autour de la table, qui selon certaines législations en vigueur ou selon les liens privilégiés qu'il partage avec l'autorité précitée, transmettra ledit résultat.

La TFL opère au niveau de l'arrondissement judiciaire et est constituée d'une composante opérationnelle et d'une composante stratégique. En fonction des nécessités, plusieurs TFL opérationnelles peuvent cependant être mises en place sur le territoire d'un arrondissement judiciaire. S'il n'y a pas de nécessité d'organiser plusieurs TFL opérationnelles, la TFL organisée traite à la fois des matières opérationnelles et stratégiques.

En ce qui concerne les missions prévues au paragraphe 2, il convient de préciser que la TFL opérationnelle assure la collecte d'informations et alimente, via un service de base, la banque de données commune T.E.R. Elle suit les entités de la banque de données commune T.E.R. présentes sur son territoire conformément à l'évaluation de la menace établie par l'Organe de Coordination pour l'Analyse de la Menace (OCAM). La TFL opérationnelle détermine les entités prioritaires et se concerte, pour chacune d'entre elles, sur le suivi et les mesures les plus appropriés. Il convient de préciser que chaque entité devra faire l'objet d'un examen au minimum deux fois par an au sein de la TFL. Et ce, afin d'en assurer un suivi optimal.

La priorisation effectuée par la TFL repose sur un certain nombre de critères soigneusement définis et s'avère nécessaire dans la mesure où certaines entités requièrent plus d'attention et de suivi que d'autres et détermine la plateforme où l'entité sera traitée.

Comme développé dans la nouvelle 'note stratégique: extrémisme et terrorisme' de l'OCAM de septembre 2021, la priorisation des entités est organisée de la manière suivante:

een bepaalde entiteit. Het doel is zo ruim mogelijk te zijn. Het doorslaggevende criterium is de bijdrage die een persoon of een dienst kan hebben voor het in de LTF bestudeerde geval.

Teneinde de werking van elke opgerichte LTF te uniformeren, voorziet artikel 32 voortaan dat de administratieve coördinatie, het secretariaat en de opvolging van de LTF worden gewaarborgd door de bestuurlijke directeur-coördinator van de federale politie of de personen die hij aanwijst, en dit teneinde die taken te kunnen delegeren. Zo kan de directeur-coördinator, bijvoorbeeld wanneer het resultaat van het overleg bedoeld in artikel 32 moet worden overgezonden aan de bevoegde overheid om de maatregel ten aanzien van de entiteit te nemen, een partner rond de tafel aanwijzen die volgens bepaalde geldende wetgevingen of volgens de bevoorrechte banden die hij deelt met bovengenoemd overheid, voornoemd resultaat zal verzenden.

De LTF is actief op het niveau van het gerechtelijk arrondissement en bestaat uit een operationele component en een strategische component. Naargelang van de behoeften kunnen evenwel verschillende operationele LTF's worden opgericht op het grondgebied van een gerechtelijk arrondissement. Indien het niet nodig is om meerdere operationele LTF's op te richten, behandelt de opgerichte LTF zowel operationele als strategische aangelegenheden.

Met betrekking tot de opdrachten bedoeld in paragraaf 2 moet worden verduidelijkt dat de operationele LTF informatie verzamelt en, via een basisdienst, de gemeenschappelijke gegevensbank T.E.R. voedt. De LTF volgt de entiteiten van de gemeenschappelijke gegevensbank T.E.R. die op zijn grondgebied aanwezig zijn overeenkomstig de dreigingsanalyse opgesteld door het Coördinatieorgaan voor de dreigingsevaluatie (OCAD). De operationele LTF bepaalt de prioritaire entiteiten en pleegt, voor elk van hen, overleg over de opvolging en de meest gepaste maatregelen. Er moet worden gespecificeerd dat elke entiteit ten minste twee keer per jaar moet worden beoordeeld binnen de TFL. En dit om een optimale opvolging te verzekeren.

De prioritering door de LTF berust op een aantal zorgvuldig bepaalde criteria en blijkt noodzakelijk aangezien bepaalde entiteiten meer aandacht en opvolging vragen dan anderen en bepaalt het platform waar de entiteit zal worden behandeld.

Zoals uiteengezet in de nieuwe 'Strategische Nota: extremisme en terrorisme' van het OCAD van september 2021, komt de prioritering van de entiteiten als volgt tot stand:

— Les entités A sont principalement suivies par la Police Judiciaire Fédérale et/ou les services de renseignement dans le cadre d'une enquête pénale classique menée par le Ministère public ou le juge d'instruction et/ou dans le cadre d'une enquête de renseignement. Les TFL sont tenues au courant des dossiers et si des mesures à prendre sont nécessaires;

— Les entités B sont, pour la plupart, suivies sur les plateformes des TFL et des partenaires qui en font parties;

— Les entités C sont, pour la plupart, l'objet d'un suivi primaire sur la plateforme CSIL-R et des partenaires qui en font partie;

— Les entités D sont, par exemple, des personnes qui séjournent en prison à l'étranger ou ont été éloignées du territoire belge. Ce critère permet de conserver l'entité dans la banque de données commune T.E.R., jusqu'à ce qu'une suppression de l'entité y soit envisagée.

Des entités peuvent donc être suivies en même temps sur différentes plateformes. Cette catégorisation ne doit pas être considérée comme statique mais comme dynamique car le suivi d'une entité peut évoluer.

En ce qui concerne la TFL stratégique, celle-ci tend à assurer la concordance entre les éventuelles TFL opérationnelles mises en place sur le territoire d'un arrondissement judiciaire.

Enfin, en ce qui concerne le cas particulier des entités placées en détention, actuellement, elles sont discutées au sein du Groupe de travail opérationnel Prisons de la Nationale task force. Ce groupe de travail est composé de la Sûreté de l'État, de l'OCAM, de la Police fédérale ainsi que de la Direction générale des Établissements Pénitentiaires du Service public fédéral Justice. Cette plateforme de discussion est chargée d'assurer l'échange des données à caractère personnel et des informations concernant les détenus qui figurent dans la banque de données commune, leur suivi et la détermination de mesures pénitentiaires appropriées à leur égard. À noter que la DG EPI inscrit les mesures dans la banque de données commune afin de les retransmettre à la TFL concernée.

Conformément à l'avis du Conseil d'État 73.442/2 du 7 juin 2023 et à l'avis de l'Autorité de protection des données 97/2023 du 16 juin 2023, il convient d'omettre l'habilitation du Roi à déterminer d'autres missions de la TFL. En effet, la TFL est une plateforme d'échange qui travaille sur base des données de la banque de données

— A-entiteiten worden in hoofdzaak opgevolgd door de Federale Gerechtelijke Politie en/of de inlichtingendiensten in het kader van een klassiek strafonderzoek onder leiding van het parket of de onderzoeksrechter en/of in het kader van een inlichtingenonderzoek. De LTF's worden op de hoogte gehouden van de dossiers en van de eventuele noodzaak om maatregelen te nemen;

— B-entiteiten krijgen voor het merendeel een opvolging via het platform van de LTF's en de bijhorende partners;

— C-entiteiten krijgen voor het merendeel hun primaire opvolging via het platform van de LIVC's-R en de bijhorende partners;

— D-entiteiten betreffen bijvoorbeeld personen die in de gevangenis in het buitenland zitten of die van het Belgische grondgebied verwijderd werden. De opname als entiteit verzekert dat de entiteit in kwestie in de gemeenschappelijke gegevensbank T.E.R. blijft tot zij verwijderd kan worden.

Entiteiten kunnen dan ook op verschillende platformen tegelijk worden opgevolgd. Die categorisering moet niet als statisch maar als dynamisch worden beschouwd aangezien de opvolging van een entiteit kan evolueren.

De strategische LTF strekt ertoe de overeenstemming tussen de eventuele operationele LTF's opgericht op het grondgebied van een gerechtelijk arrondissement, te waarborgen.

Tot slot wordt het specifieke geval van de entiteiten die in hechtenis zijn genomen, momenteel besproken in de operationele werkgroep Gevangenen van de nationale taskforce. Deze werkgroep bestaat uit de Veiligheid van de Staat, het OCAD, de federale politie en het directoraat-generaal Penitentiare Inrichtingen van de Federale Overheidsdienst Justitie. Dit discussieplatform is belast met het verzekeren van de uitwisseling van persoonsgegevens en informatie over gedetineerden die in de gemeenschappelijke gegevensbank zijn opgenomen, hun follow-up en de vaststelling van passende gevangenis maatregelen voor hen. Er moet worden opgemerkt dat het DG EPI de maatregelen in de gemeenschappelijke gegevensbank invoert, teneinde terug te kunnen koppelen naar de betrokken LTF's.

Overeenkomstig advies nr. 73.442/2 van 7 juni 2023 van de Raad van State en advies nr. 97/2023 van 16 juni 2023 van de Gegevensbeschermingsautoriteit moet de machtiging van de Koning om andere opdrachten van de LTF te bepalen, worden weggelaten. De LTF is namelijk een uitwisselingsplatform dat werkt met de

commune dont les traitements sont ceux prévus dans le cadre de la banque de données.

Art. 33

À l'article 33, afin d'assurer le suivi de l'entité validée enregistrée dans la banque de données commune T.E.R., le législateur prévoit, désormais, que la TFL se concerta systématiquement sur l'opportunité de prendre ou non une ou plusieurs mesures à l'égard de l'entité validée, sans préjudice des prérogatives des autorités compétentes pour prendre la mesure.

Il est prévu que cette concertation ait lieu à deux moments:

- dès la validation d'une entité dans la banque de données commune et sur base des données à caractère personnel et des informations visées à l'article 31;
- dans le cadre du suivi d'une entité validée, lorsque de nouvelles données à caractère personnel et informations visées à l'article 31 peuvent entraîner un changement de mesures.

Dans un souci de suivi optimal de l'entité enregistrée, il est prévu que le résultat de cette concertation soit transmis aux autorités compétentes pour prendre les mesures.

Ces dernières conservent leurs prérogatives en ce qui concerne l'examen de la prise de mesures mais le résultat de la concertation de la TFL est un élément non contraignant qui peut être pris en considération lors de l'examen de la prise de mesures par l'autorité compétente.

Chaque autorité compétente pour prendre une mesure garde donc sa compétence exclusive pour le faire et ce, quand elle le souhaite. Elle n'est dès lors pas tributaire de la tenue d'une TFL. La TFL reste une plateforme de discussion et d'échange qui n'a pour objectif que d'attirer l'attention de l'autorité compétente sur ce que pensent les partenaires autour de la table de la prise ou non d'une mesure. À cet égard, l'Autorité de protection des données (avis 97/2023 du 16 juin 2023, § 90) et le Comité R (avis du 13 juillet 2023, § 32) n'ont pas une bonne lecture des textes. En effet, le projet ne conditionne pas les compétences des services qui doivent prendre les mesures et il n'est pas question pour la TFL de se substituer à ces services. Le résultat de la concertation en TFL au sujet des mesures ne constitue pour le service habilité à prendre les mesures qu'un

gegevens van de gemeenschappelijke gegevensbank waarvan de verwerking die is die wordt bepaald binnen het kader van de gegevensbank.

Art. 33

In artikel 33 voorziet de wetgever, met het oog op de opvolging van de in de gemeenschappelijke gegevensbank T.E.R. opgenomen gevalideerde entiteit, voortaan erin dat de LTF stelselmatig overleg pleegt over de opportuniteit om al dan niet een of meer maatregelen te nemen ten aanzien van de gevalideerde entiteit, onverminderd de prerogatieven van de overheden die bevoegd zijn om de maatregel te nemen.

Dat overleg wordt op twee tijdstippen gepland:

- vanaf de validering van een entiteit in de gemeenschappelijke gegevensbank en op grond van de persoonsgegevens en de informatie bedoeld in artikel 31;
- in het kader van de opvolging van een gevalideerde entiteit, wanneer nieuwe persoonsgegevens en informatie bedoeld in artikel 31 tot een wijziging van maatregelen kunnen leiden.

Met het oog op een optimale opvolging van de opgenomen entiteit wordt bepaald dat het resultaat van dat overleg wordt bezorgd aan de overheden die bevoegd zijn om de maatregelen te nemen.

Zij behouden hun prerogatieven met betrekking tot het onderzoek van het nemen van maatregelen, maar het resultaat van het overleg van de LTF is een niet-bindend element dat in overweging kan worden genomen wanneer de bevoegde overheid het nemen van maatregelen onderzoekt.

Elke overheid die bevoegd is om een maatregel te nemen, behoudt dus haar exclusieve bevoegdheid om dit te doen, wanneer zij dat wenst. Zij is derhalve niet afhankelijk van de houding van een LTF. De LTF blijft een platform voor discussie en uitwisseling, met als enig doel de aandacht van de bevoegde autoriteit te vestigen op wat de partners rond de tafel denken over de vraag of een maatregel al dan niet moet worden genomen. In dat opzicht is er een verkeerde lezing van de tekst door de Gegevensbeschermingsautoriteit (advies nr. 97/2023 van 16 juni 2023, § 90) en Comité I (advies van 13 juli 2023, § 32). In het ontwerp worden namelijk geen voorwaarden gesteld aan de bevoegdheden van de diensten die de maatregelen nemen, en het is niet de bedoeling dat de LTF in de plaats komt van die diensten. Het resultaat van het overleg in de LTF

élément supplémentaire parmi les autres éléments dont il dispose dans son dossier. Il ne s'agit dès lors pas d'un avis obligatoire. Et comme indiqué ci-avant, le service compétent ne doit pas attendre qu'une TFL se soit réunie pour prendre une mesure qu'il estime nécessaire. Il conserve sa prérogative à tout moment.

Par ailleurs, dans son avis, le Comité R estime que la disposition crée une différence de traitement entre les personnes présentes dans la B.D.C. T.E.R. et les autres, dès lors que dans le premier cas, toute autorité exerçant son pouvoir d'appréciation dans le cadre de la prise d'un acte administratif ou d'une décision doit satisfaire à une condition supplémentaire par rapport au second cas (la prise en considération du résultat de la concertation) (§ 32). Or, cette disposition traite différemment des choses différentes. La différence de traitement se fonde sur un critère objectif, à savoir la présence ou non d'une entité dans la banque de données commune T.E.R.

Sur base de la recommandation du Comité R (avis du 13 juillet 2023, § 33), le résultat de la concertation en T.F.L., à propos d'une entité doit être enregistrée dans la banque de données commune T.E.R. à des fins de bonne exécution, de transparence et de contrôle. Cependant, si la mesure est sous embargo ou classifiée (par exemple car il s'agit d'une mesure BIM) elle ne sera pas enregistrée.

L'article 33 prévoit également une liste non exhaustive des mesures qui doivent systématiquement faire l'objet d'une concertation au sein de la TFL, mais elle constitue une liste "a minima" des mesures à discuter. Ainsi, si cela s'avère nécessaire, des mesures supplémentaires peuvent également être abordées lors de la TFL.

Les mesures "a minima" qui doivent faire l'objet d'une concertation au sein de la TFL sont:

1° la mesure de signalement et de désignement.

Plusieurs signalements sont visés: le signalement policier, le signalement de renseignement, le signalement par l'Office des étrangers, conformément aux réglementations respectives en vigueur, ou encore le signalement dans le cadre de la réglementation belge relative au traitement des données des passagers.

Il s'agit notamment:

a) des articles 26, 32, 34, 36, 38 et 40 du règlement (UE) 2018/1862 du Parlement européen et du Conseil

over de maatregelen komt voor de dienst gemachtigd om de maatregelen te nemen dus louter bij de andere elementen te zijner beschikking in zijn dossier. Dat wil dus zeggen dat het geen verplicht advies is. Zoals hierboven aangegeven, hoeft de bevoegde dienst de vergadering van de LTF niet af te wachten om een maatregel naar eigen goeddunken te nemen. Hij behoudt te allen tijde zijn voorrecht.

In zijn advies meent Comité I dat de bepaling een verschil in behandeling creëert tussen de personen aanwezig in de gemeenschappelijke gegevensbank T.E.R. en de anderen, aangezien in het eerste geval elke autoriteit die haar beoordelingsbevoegdheid uitoefent in de context van het nemen van een administratieve handeling of een beslissing moet voldoen aan een extra voorwaarde in vergelijking met het tweede geval (het rekening houden met het resultaat van het overleg) (§ 32). Deze bepaling handelt echter op verschillende wijzen over verschillende zaken. Het verschil in behandeling berust op een objectief criterium, namelijk het feit of een entiteit al dan niet aanwezig is in de gemeenschappelijke gegevensbank T.E.R.

Volgens de aanbeveling van Comité I (advies van 13 juli 2023, § 33) moet het resultaat van het overleg in de LTF over een entiteit met het oog op een goede uitvoering, transparantie en controle worden vermeld in de gemeenschappelijke gegevensbank T.E.R. Als de maatregel echter onder embargo staat of geclassificeerd is (bijvoorbeeld omdat het een BIM-maatregel is), wordt deze niet opgenomen.

In artikel 33 wordt eveneens voorzien in een niet-exhaustieve lijst van maatregelen waarover systematisch moet worden overlegd binnen de LTF, maar het betreft een "minimale" lijst van de te bespreken maatregelen. Zo kunnen er, indien zulks nodig blijkt, bij de LTF eveneens aanvullende maatregelen worden besproken.

De minimale maatregelen waarover moet worden overlegd binnen de LTF, zijn:

1° de maatregel van seining en ontseining.

Er worden verschillende seiningen beoogd: de positionele seining, de inlichtingseining, de seining door de Dienst Vreemdelingenzaken, overeenkomstig de respectievelijke geldende regelgevingen, en de seining in het kader van de Belgische regelgeving betreffende de verwerking van passagiersgegevens.

Deze omvatten met name:

a) artikelen 26, 32, 34, 36, 38 et 40 van de Verordening (EU) 2018/1862 van het Europees Parlement en de Raad

du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) n° 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission;

b) de l'article 3 du règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier;

c) de l'article 24 du règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) no 1987/2006;

d) de la réglementation d'Interpol;

e) des articles 44/5 et 44/7 de la loi sur la fonction de police.

2° la suspension, le retrait et la restitution de cartes d'identification ou la suspension et le retrait d'autorisations qui relèvent du champ d'application de la loi du 19 juillet 1991 organisant la profession de détective privé et de la loi du 2 octobre 2017 réglementant la sécurité privée et particulière.

Sont ici visées les autorisations accordées aux entreprises de gardiennage, entreprises de consultance en sécurité, services internes de gardiennage et de détectives privés, les agréments pour les entreprises de sécurité et les chargés de cours dans les organismes de formation ainsi que les autorisations pour le personnel de travailler dans ce secteur. Il en va de même pour les permis d'armes octroyés aux agents de gardiennage.

3° le retrait, la suspension ou la limitation d'autorisations ou d'agréments qui relèvent du champ d'application de la loi du 8 juin 2006 réglant les activités économiques et individuelles avec des armes.

4° le retrait d'habilitations, attestations et avis de sécurité qui relèvent du champ d'application de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

van 28 november 2018 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van politieke en justitiële samenwerking in strafzaken, tot wijziging en intrekking van Besluit 2007/533/JBZ van de Raad en tot intrekking van Verordening (EG) nr. 1986/2006 van het Europees Parlement en de Raad en Besluit 2010/261/EU van de Commissie;

b) artikel 3 van de Verordening (EU) 2018/1860 van het Europees Parlement en de Raad van 28 november 2018 betreffende het gebruik van het Schengeninformatiesysteem voor de terugkeer van illegaal verblijvende onderdanen van derde landen;

c) artikel 24 van de Verordening (EU) 2018/1861 van het Europees parlement en de Raad van 28 november 2018 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van grenscontroles, tot wijziging van de Overeenkomst ter uitvoering van het Akkoord van Schengen en tot wijziging en intrekking van Verordening (EG) nr. 1987/2006.

d) Interpol regelgeving;

e) artikelen 44/5 en 44/7 van de wet op het politieambt.

2° de schorsing, de intrekking en de teruggave van identificatiekaarten of de schorsing en de intrekking van vergunningen die behoren tot het toepassingsgebied van de wet van 19 juli 1991 tot regeling van het beroep van privédetective en de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid.

Hier worden bedoeld de vergunningen toegekend aan bewakingsondernemingen, ondernemingen voor veiligheidsadvies, interne bewakingsdiensten en privédetectives, de erkenningen voor beveiligingsondernemingen en lesgevers in opleidingsinstellingen alsmede de vergunningen voor het personeel om in die sector te werken. Hetzelfde geldt voor de wapenvergunningen toegekend aan bewakingsagenten.

3° de intrekking, de schorsing of de beperking van de vergunningen of de erkenningen die behoren tot het toepassingsgebied van de wet van 8 juni 2006 houdende regeling van economische en individuele activiteiten met wapens.

4° de intrekking van veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen die behoren tot het toepassingsgebied van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

5° la mise en place d'une enquête sociale et fiscale ou toute autre mesure spécifique dans les limites des compétences légales du Service d'information et de recherche sociale du Service public fédéral Emploi, Travail et Concertation Sociale.

Le Service d'information et de recherche sociale se chargera à son tour de soutenir et de coordonner les actions nécessaires des services fédéraux dans la lutte contre la fraude sociale.

6° la mise en place d'une enquête financière par la Cellule de Traitement des Informations Financières (CTIF) conformément à l'article 81, § 2 et l'article 83, § 2, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme.

La CTIF peut entamer une enquête financière conformément à l'article 81, § 2, et l'article 83, § 2, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme, à la demande de la Sûreté de l'État, le SGRS et l'OCAM dans le cadre de la lutte contre le terrorisme, le financement du terrorisme et les opérations de blanchiment qui pourraient y être liées et conformément à l'article 79, § 3, 2°, de la même loi sur la base des informations communiquées par le ministère public dans le cadre d'une enquête pénale en lien avec le financement du terrorisme.

7° la prise de mesures spécifiques dans les limites des compétences légales des services de l'ONEM, du FOREM, d'ACTIRIS, VDAB et ADG.

8° la prise de mesures spécifiques par l'Office des étrangers en matière d'accès au territoire, de séjour, d'établissement et d'éloignement.

Pour chaque entité enregistrée dans la banque de données commune T.E.R., l'Office des étrangers procède à une analyse afin de prendre les mesures adéquates. Par exemple, en ce qui concerne l'accès au territoire, la demande de visa peut être examinée. En ce qui concerne le séjour, c'est le dossier individuel qui peut être examiné.

9° le refus, le retrait ou l'invalidation de passeport ou d'un titre de voyage belge et de documents d'identité belge conformément au Code consulaire.

10° l'inscription d'office ou la radiation d'office des registres de la population conformément à la loi du 19 juillet 1991 relative aux registres de la population, aux cartes

5° de l'uitvoering van een sociaal en fiscaal onderzoek of enige andere specifieke maatregel binnen de grenzen van de wettelijke bevoegdheden van de Sociale Inlichtingen- en Opsporingsdienst van de Federale Overheidsdienst Werkgelegenheid, Arbeid en Sociaal Overleg.

De Sociale Inlichtingen- en Opsporingsdienst is op zijn beurt belast met de ondersteuning en coördinatie van de nodige acties vanwege de federale diensten ter bestrijding van sociale fraude.

6° de l'uitvoering van een financieel onderzoek door de Cel voor Financiële Informatieverwerking (CFI) overeenkomstig artikel 81, § 2, en artikel 83, § 2, van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten.

De CFI kan een financieel onderzoek opstarten overeenkomstig artikel 81, § 2, en artikel 83, § 2, van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten, op verzoek van de Veiligheid van de Staat, de ADIV en het OCAD in het kader van de bestrijding van terrorisme, van financiering van terrorisme en van de witwasverrichtingen die ermee verband zouden kunnen houden, alsook overeenkomstig artikel 79, § 3, 2°, van diezelfde wet, op basis van de informatie meegedeeld door het openbaar ministerie in het kader van een strafonderzoek in verband met de financiering van terrorisme.

7° het nemen van specifieke maatregelen binnen de grenzen van de wettelijke bevoegdheden van de diensten van de RVA, FOREM, Actiris, VDAB en ADG.

8° het nemen van specifieke maatregelen door de Dienst Vreemdelingenzaken op het gebied van toegang tot het grondgebied, verblijf, vestiging en verwijdering.

Voor elke entiteit die in de gemeenschappelijke gegevensbank T.E.R. is opgenomen, voert de Dienst Vreemdelingenzaken een analyse uit teneinde passende maatregelen te nemen. Voor wat de toegang tot het grondgebied betreft, kan bijvoorbeeld de visumaanvraag worden onderzocht. Voor wat het verblijf betreft, kan het individuele dossier worden onderzocht.

9° de weigering, de intrekking of de ongeldigverklaring van een Belgisch paspoort of reisdocument en van Belgische identiteitsdocumenten overeenkomstig het Consulaire Wetboek.

10° het van ambtswege inschrijven of schrappen uit de bevolkingsregisters overeenkomstig de wet van 19 juli 1991 betreffende de bevolkingsregisters,

d'identité, aux cartes d'étranger et aux documents de séjour.

S'il s'avère qu'une personne ne séjourne plus à l'adresse à laquelle elle est inscrite dans les registres de la population et s'il est impossible de constater sa nouvelle résidence principale, le Collège des bourgmestres et échevins peut décider de radier d'office cette personne des registres.

11° le gel des avoirs en application de l'arrêté royal du 28 décembre 2006 relatif aux mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le financement du terrorisme.

Le Conseil des ministres inscrit, sur l'avis du Conseil national de sécurité, l'entité qui a commis ou tenté de commettre un acte terroriste, sur la liste nationale des personnes dont les fonds et les ressources économiques sont gelés, en concertation avec les services d'appui concernés et après approbation de l'autorité judiciaire compétente (le parquet fédéral).

12° le suivi effectué par les services de police dans le cadre des missions visées aux articles 14 et 15, de la loi sur la fonction de police.

13° le suivi effectué par les services de renseignements dans le cadre des missions visées aux articles 7 et 11, de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité.

Le suivi effectué par les services de police dont il est question à l'alinéa précédent peut être précédé ou complété par un suivi effectué par les services de renseignement.

14° le suivi des médias sociaux de l'entité concernée.

Le suivi des médias sociaux consiste à examiner si l'entité est active sur les réseaux sociaux et le cas échéant, y identifier ses activités.

15° les mesures visées dans le Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne et le Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques.

de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten.

Indien blijkt dat een persoon niet langer verblijft op het adres waarop hij in de bevolkingsregisters ingeschreven staat, en indien het onmogelijk is zijn nieuwe hoofdverblijfplaats vast te stellen, kan het college van burgemeester en schepenen beslissen deze persoon van ambtswege uit de registers te schrappen.

11° de bevrozing van tegoeden met toepassing van het koninklijk besluit van 28 december 2006 inzake specifieke beperkende maatregelen tegen bepaalde personen en entiteiten met het oog op de strijd tegen de financiering van het terrorisme.

De Ministerraad neemt, op advies van de Nationale Veiligheidsraad, de entiteit die een terroristische daad heeft gesteld of gepoogd heeft te stellen, op in de nationale lijst van de personen van wie de tegoeden en economische middelen zijn bevroren, in overleg met de betrokken steundiensten en na goedkeuring van de bevoegde gerechtelijke overheid (het federaal parket).

12° de opvolging uitgevoerd door de politiediensten in het kader van de opdrachten bedoeld in de artikelen 14 en 15 van de wet op het politieambt.

13° de opvolging uitgevoerd door de inlichtingendiensten in het kader van de opdrachten bedoeld in de artikelen 7 en 11 van de organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

De opvolging uitgevoerd door de politiediensten waarvan in het vorige lid sprake is, kan worden voorafgegaan door of aangevuld met een opvolging uitgevoerd door de inlichtingendiensten.

14° de opvolging van de sociale media van de betrokken entiteit.

De opvolging van de sociale media bestaat erin te onderzoeken of de entiteit actief is op de sociale netwerken en, in voorkomend geval, zijn activiteiten in kaart te brengen.

15° de maatregelen bedoeld in Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud en Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eenge maakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (digitaal dienstenverordening).

Cette mesure a été ajoutée suite à l'avis du Comité permanent R (§ 34).

CHAPITRE 4

Dispositions modificatives

Section 1^{er}

Dispositions modificatives de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

Les modifications apportées à la loi relative à la protection des données par les articles 34 à 50 s'inscrivent dans la lignée du principe énoncé à l'article 4.

Ainsi, le présent projet de loi règle les questions en matière de protection des données qui sont propres aux traitements de données au sein de la banque de données commune T.E.R., à savoir quels types de données à caractère personnel y sont traitées, pour quelles finalités, pendant combien de temps, qui est responsable du traitement, quelles autorités doivent alimenter la banque de données, avec quelles catégories de données, quelles sont les catégories d'autorités qui peuvent recevoir accès ou communication de tout ou partie des données, l'obligation de journaliser les données, et quelles sont les autorités de protection des données compétentes.

Par ailleurs, dans une optique de cohérence, le législateur a choisi pour les autres règles en matière de protection des données (obligation des responsables du traitement, choix d'un sous-traitant, droits des personnes concernées, ...) de se raccrocher au titre 3, sous-titre 4, de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, qui est dédié aux traitements de données à caractère personnel réalisés par l'OCAM. Toute proportion gardée, on retrouve en effet une similitude entre les traitements que l'OCAM effectue sur des données à caractère personnel et des informations provenant de ses différents services d'appui avec la banque de données commune T.E.R. qui mutualise les données à caractère personnel et les informations introduites par les services de bases et d'autres partenaires. Le traitement "en commun" des données dans la banque de données commune T.E.R. implique qu'un seul régime commun soit appliqué à ces données, en particulier concernant le droit des personnes concernées, ceci au bénéfice d'une plus grande sécurité juridique profitable à tous.

Die maatregel werd toegevoegd ingevolge het advies van Vast Comité I (§ 34).

HOOFDSTUK 4

Wijzigingsbepalingen

Afdeling 1

Wijzigingsbepalingen van de wet van 30 juli 20178 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens

De wijzigingen van de wet op de gegevensbescherming aangebracht door de artikelen 34 tot en met 50 zijn in overeenstemming met het beginsel van artikel 4.

Dit wetsontwerp regelt dus de gegevensbeschermingskwesaties die specifiek zijn voor de verwerking van gegevens in de gemeenschappelijke gegevensbank T.E.R., namelijk welke soorten persoonsgegevens daar worden verwerkt, voor welke doeleinden, hoe lang, wie verantwoordelijk is voor de verwerking, welke autoriteiten de databank moeten voeden, met welke categorieën gegevens, welke categorieën autoriteiten toegang kunnen krijgen tot of mededeling kunnen doen van alle of een deel van de gegevens, de verplichting om de gegevens vast te leggen, en welke gegevensbeschermingsautoriteiten bevoegd zijn.

Voorts heeft de wetgever met het oog op de samenhang ervoor gekozen om de andere regels inzake gegevensbescherming (verplichting van de voor de verwerking verantwoordelijken, keuze van een verwerker, rechten van de betrokkenen, ...) te relateren aan titel 3, subtitel 4, van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, die gewijd is aan de verwerking van persoonsgegevens door het OCAD. Relatief gezien is er namelijk een gelijkenis tussen de door het OCAD uitgevoerde verwerkingen van persoonsgegevens en informatie afkomstig van zijn verschillende steundiensten en de gemeenschappelijke gegevensbank T.E.R. die de persoonsgegevens en informatie ingevoerd door de basisdiensten en andere partners mutualiseert. Voorts impliceert de "gezamenlijke" verwerking van gegevens in de gemeenschappelijke gegevensbank T.E.R. dat er één gemeenschappelijke regeling wordt toegepast op deze gegevens, met name wat de rechten van de betrokkenen betreft, zulks ten behoeve van een grotere rechtszekerheid voor iedereen.

Comme le fait remarquer le Conseil d'État dans son avis 73.442/2 du 7 juin 2023 et le Comité R dans son avis du 13 juillet 2023 (§ 3), un certain nombre de dispositions de l'avant-projet semble faire double emploi avec le régime applicable au traitement des données à caractère personnel prévu au titre 3, sous-titre 4 de la loi relative à la protection des données. L'auteur de l'avant-projet reconnaît que la remarque est juste et a corrigé le projet en réalisant une plus grande intégration des règles applicables en matière de traitement de données à caractère personnel dans le titre 3, sous-titre 4 précité. C'est ainsi que la partie modificative de la loi relative à la protection des données a été enrichie afin que tous les aspects des traitements de données à caractère personnel de la banque de données commune T.E.R. soient bel et bien visés dans la loi précitée.

En ce qui concerne l'ancien article 29 de l'avant-projet, bien que l'auteur ne partage pas le point de vue du Conseil d'État qui considère la disposition comme faisant doublon avec l'article 157 de la loi sur la protection des données, il a néanmoins jugé pertinent d'inscrire dans la loi précitée le régime applicable au délégué à la protection des données de la banque de données commune T.E.R. L'article 29 ancien a par conséquent été retiré du projet.

En définitive, le régime général en matière de traitement de données à caractère personnel pour la banque de données commune T.E.R. se trouve entièrement intégrée dans la loi sur la protection des données. L'avant-projet ne contient plus que des aménagements, comme les délais de conservation des données et les brèches de sécurité ou des règles spécifiques à certains acteurs de la banque de données commune (notamment le gestionnaire et le responsable opérationnel).

Dans son avis n° 97/2023 du 16 juin 2023, l'Autorité de protection des données rappelle qu' "une autorité publique est en principe responsable du traitement de données nécessaire à la mise en œuvre de la mission d'intérêt public qui lui incombe, ou qui relève de l'autorité publique dont elle est investie, en vertu de la législation concernée. Cela implique de préciser très clairement de quelle(s) autorité(s) relève la BDC (ou auprès de quelles autorités la BDC est instituée) et pourquoi. Une disposition adéquatement libellée à cet égard doit permettre de déterminer: (...) quel Titre de la LPD est applicable au traitement des données à caractère personnel effectué sous la responsabilité des responsables du traitement de la BDC" (§§ 107-108).

Zoals opgemerkt door de Raad van State in advies nr. 73.442/2 van 7 juni 2023 en door Comité I in het advies van 13 juli 2023 (§ 3) blijken een aantal bepalingen van het voorontwerp te overlappen met de regels die van toepassing zijn op de in titel 3, ondertitel 4, van de wet gegevensbescherming bedoelde verwerking van persoonsgegevens. De auteur van het voorontwerp erkent dat de opmerking terecht is en heeft het ontwerp verbeterd door de in titel 3, ondertitel 4, van de voornoemde wet bedoelde regels van toepassing op de verwerking van persoonsgegevens in ruimere mate erin op te nemen. Op die manier werd het wijzigende gedeelte van de wet gegevensbescherming verrijkt, zodat alle facetten van de verwerking van persoonsgegevens in de gemeenschappelijke gegevensbank T.E.R. effectief worden beoogd in de voornoemde wet.

Met betrekking tot het oude artikel 29 van het voorontwerp achtte de auteur, hoewel hij het standpunt van de Raad van State dat de bepaling overlapt met artikel 157 van de wet gegevensbescherming niet deelt, het wel relevant om de regels van toepassing op de functionaris voor gegevensbescherming van de gemeenschappelijke gegevensbank T.E.R. in de voornoemde wet op te nemen. Het oude artikel 29 werd bijgevolg uit het ontwerp gehaald.

Tot slot is de algemene regeling inzake de verwerking van persoonsgegevens voor de gemeenschappelijke gegevensbank T.E.R. volledig opgenomen in de wet gegevensbescherming. Het voorontwerp bevat enkel nog aanpassingen, zoals de bewaartermijn voor gegevens en de inbreuken op de beveiliging, of specifieke regels voor bepaalde actoren van de gemeenschappelijke gegevensbank (met name de beheerder en de operationeel verantwoordelijke).

In advies nr. 97/2023 van 16 juni 2023 wijst de Gegevensbeschermingsautoriteit erop "dat een overheidsinstantie in beginsel verantwoordelijk is voor de verwerking van gegevens die noodzakelijk is voor de vervulling van de haar toevertrouwde openbare opdracht of die krachtens de betrokken wetgeving binnen de werkingssfeer van het aan haar toevertrouwde openbaar gezag valt. Dit betekent dat heel duidelijk moet worden gemaakt aan welke overheid/overheden de GGB rapporteert (of bij welke overheid/overheden de GGB is opgericht) en waarom. Een goed geformuleerde bepaling in dit verband moet het mogelijk maken om te bepalen: [...] welke titel van de [wet gegevensbescherming] van toepassing is op de verwerking van persoonsgegevens die wordt uitgevoerd onder de verantwoordelijkheid van de verwerkingsverantwoordelijken van de GGB" (§§ 107- 108).

Concernant la remarque de l'Autorité de protection des données, il est tout d'abord rappelé que la disposition de l'article 30 entend justement répondre à cette interrogation. Il est renvoyé pour les détails au commentaire dudit article. Ensuite, la remarque de l'Autorité de protection des données nous permet de repréciser ce que le dispositif de l'avant-projet met en place. L'avant-projet désigne, sans équivoque possible, les responsables du traitement de la banque de données commune à l'article 5, alinéa 1^{er}. Ces responsables du traitement sont ceux qui se voient attribuer la responsabilité de la mise en œuvre des dispositions contenues dans la loi sur la protection des données, telles que modifiées par l'avant-projet. Là encore, aucun doute n'est permis quant au contour des responsabilités des responsables du traitement des données à caractère personnel de la banque de données commune: les modifications apportées à la loi précitée ne concernent que "les responsables conjoints du traitement de la banque de données commune T.E.R." (l'avant-projet de loi, dans sa partie modificative de la loi sur la protection des données apporte la définition suivante des responsables conjoints du traitement de la BDC: "les responsables du traitement visé à l'article 5, alinéa 1^{er}, de la loi du XXX portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation", étant entendu que la loi du XXX précitée est le présent avant-projet de loi). L'auteur du projet ne voit donc pas comment il pourrait formuler plus clairement ce libellé.

Le commentaire de l'Autorité de protection des données, nous invite à repréciser que le contexte de la banque de données commune T.E.R. connaît deux acteurs à côté du responsable du traitement dont les rôles constituent une originalité par rapport au RGPD. Dans la banque de données commune T.E.R., la gestion des données à caractère personnel implique trois acteurs: les responsables conjoints du traitement, au sens de la loi relative à la protection des données et du RGPD, ainsi que le gestionnaire et le responsable opérationnel. En principe donc la mise en œuvre et le respect des principes du traitement des données à caractère personnel incombent aux responsables conjoints du traitement de la banque de données commune T.E.R. L'avant-projet de loi spécifie cependant quelques règles de traitement dont la responsabilité incombe au gestionnaire et au responsable opérationnel. Il en est ainsi, par exemple, de la gestion des brèches de sécurité (art. 13) et du contrôle de la qualité des données traitées au sein de la banque de données commune T.E.R. (art. 12, al. 2, 1^o).

Met betrekking tot de opmerking van de Gegevensbeschermingsautoriteit moet er eerst en vooral op worden gewezen dat de bepaling van artikel 30 er juist toe strekt aan die bedenking toe te komen. Voor een nadere toelichting wordt er verwezen naar de bespreking van dat artikel. Voorts kunnen we in het licht van de opmerking van de Gegevensbeschermingsautoriteit opnieuw verduidelijken wat er in de bepaling van het voorontwerp wordt ingevoerd. De verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank worden in artikel 5, eerste lid, van het voorontwerp onduidelijk aangewezen. Die verwerkingsverantwoordelijken krijgen de verantwoordelijkheid toegekend om de bepalingen in de wet gegevensbescherming, zoals gewijzigd bij het voorontwerp, ten uitvoer te leggen. Ook daar is geen twijfel mogelijk over de draagwijdte van de verantwoordelijkheden van de verantwoordelijken voor de verwerking van persoonsgegevens in de gemeenschappelijke gegevensbank: de aan de voornoemde wet aangebrachte wijzigingen hebben louter betrekking op "de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank T.E.R." (in het gedeelte van het voorontwerp van wet waarin de wet gegevensbescherming wordt gewijzigd, worden de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank omschreven als "de verwerkingsverantwoordelijken bedoeld in artikel 5, eerste lid, van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.")", met dien verstande dat de voornoemde wet van xx dit voorontwerp van wet is. De auteur van het ontwerp ziet dus niet in hoe hij die formulering duidelijker zou kunnen maken.

Gelet op de opmerking van de Gegevensbeschermingsautoriteit willen wij graag opnieuw toelichten dat er in de context van de gemeenschappelijke gegevensbank T.E.R. naast de verwerkingsverantwoordelijke twee actoren zijn met nieuwe rollen ten opzichte van de AVG. In de gemeenschappelijke gegevensbank T.E.R. zijn er drie actoren betrokken bij het beheer van de persoonsgegevens: de gezamenlijke verwerkingsverantwoordelijken in de zin van de wet gegevensbescherming en de AVG, alsook de beheerder en de operationeel verantwoordelijke. In principe zijn het dus de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank T.E.R. die verantwoordelijk zijn voor de tenuitvoerlegging en naleving van de beginselen van de verwerking van persoonsgegevens. In het voorontwerp van wet worden echter een aantal verwerkingsregels gespecificeerd waarvoor de beheerder en de operationeel verantwoordelijke verantwoordelijk zijn. Dat is bijvoorbeeld het geval voor het beheer van inbreuken op de beveiliging (artikel 13) en de controle van de kwaliteit van de in de gemeenschappelijke gegevensbank T.E.R. verwerkte gegevens (artikel 12, tweede lid, 1^o).

À noter que suite à l'avis n° 97/2023 de l'Autorité de protection des données (§§ 20-21), la modification de l'article 146 de la loi relative à la protection des données a été supprimée. Cela rend dès lors sans objet la remarque du Comité R (avis du 13 juillet 2023, § 35).

Art. 34

Cet article modifie le renvoi à la loi sur la fonction de police visé l'article 11, § 1^{er}, 2^o, de la loi relative à la protection des données, par le renvoi à la nouvelle disposition correspondante. Il s'agit d'une adaptation technique.

Art. 35

Pour les raisons évoqués ci-avant, le sous-titre 4, du Titre 3, de la loi relative à la protection des données, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par l'OCAM, est complété par une référence à la banque de données commune T.E.R.

Art. 36

Cet article ajoute des nouvelles définitions à la liste des définitions propres au sous-titre 4, du Titre 3, de la loi relative à la protection des données, à savoir:

- loi du [DATE] portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.")
- banque de données commune "T.E.R."
- responsables conjoints du traitement de la banque de données commune T.E.R.

Art. 37

L'article 139 de la loi relative à la protection des données concerne le champ d'application du sous-titre 4, du Titre 3, de la même loi. Pour les raisons évoquées ci-avant, le champ d'application est étendu à la banque de données commune T.E.R.

Ook moet er worden opgemerkt dat de wijziging van artikel 146 van de wet gegevensbescherming is geschrapt ingevolge advies nr. 97/2023 van de Gegevensbeschermingsautoriteit (§§ 20-21). Daardoor is de opmerking van Comité I (advies van 13 juli 2023, § 35) niet meer van toepassing.

Art. 34

In dit artikel wordt de verwijzing in artikel 11, § 1, 2^o van de wet gegevensbescherming naar de wet op het politieambt vervangen door de verwijzing naar de nieuwe overeenstemmende bepaling. Het betreft een technische aanpassing.

Art. 35

Om de voornoemde redenen wordt titel 3, ondertitel 4, van de wet gegevensbescherming betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door het coördinatieorgaan voor de dreigingsanalyse aangevuld met een verwijzing naar de gemeenschappelijke gegevensbank T.E.R.

Art. 36

In dit artikel worden er nieuwe definities toegevoegd aan de lijst met specifieke definities voor titel 3, ondertitel 4, van de wet gegevensbescherming, namelijk:

- de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.");
- de gemeenschappelijke gegevensbank "T.E.R.";
- de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R."

Art. 37

Artikel 139 van de wet gegevensbescherming heeft betrekking op het toepassingsgebied van titel 3, ondertitel 4, van diezelfde wet. Om de voornoemde redenen wordt het toepassingsgebied verruimd naar de gemeenschappelijke gegevensbank T.E.R.

Art. 38

L'article 140 de la loi relative à la protection des données décrit les cas dans lesquels le traitement de données à caractère personnel est légitime.

Outre les cas déjà visés, le traitement de données à caractère personnel est légitime lorsqu'il est utile dans le cadre des finalités prévues à l'article 5, alinéa 2, de la loi du [DATE] portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.").

Art. 39

Dans l'article 143 de la loi relative à la protection des données, relatif à la conservation des données à caractère personnel, le renvoi à la loi sur la fonction de police est remplacé par le renvoi à la nouvelle disposition correspondante. Il s'agit d'une adaptation technique.

Art. 40

L'article 147 de la loi relative à la protection des données concerne la tenue d'un journal des demandes d'exercice des droits par les personnes concernées.

Cet article est complété afin d'attribuer cette tâche aux responsables conjoints du traitement de la banque de données commune "T.E.R." dans le cadre des traitements effectués dans la banque de données commune "T.E.R.".

Art. 41

L'article 149 de la loi relative à la protection des données détermine certaines obligations pour le responsable du traitement. Il doit ainsi veiller à ce que l'accès aux données à caractère personnel et les possibilités de traitement soient limités à ce qui est utile dans le cadre des finalités de la banque de données commune "T.E.R." visées à l'article 5, alinéa 2, de la loi du [DATE] portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.").

Art. 42

L'article 155 concerne la gestion des brèches de sécurité. Cet article est modifié afin de tenir compte des règles particulières de gestion des brèches de sécurité

Art. 38

Artikel 140 van de wet gegevensbescherming beschrijft in welke gevallen een verwerking van persoonsgegevens rechtmatig is.

Behoudens de reeds beoogde gevallen is de verwerking van persoonsgegevens legitiem wanneer ze nuttig is in het kader van de doeleinden bedoeld in artikel 5, tweede lid, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.").

Art. 39

In artikel 143 van de wet gegevensbescherming betreffende de bewaring van persoonsgegevens wordt de verwijzing naar de wet op het politieambt vervangen door de verwijzing naar de nieuwe overeenstemmende bepaling. Het betreft een technische aanpassing.

Art. 40

Artikel 147 van de wet gegevensbescherming heeft betrekking op het bijhouden van een logbestand van alle aanvragen van betrokkenen tot uitoefening van hun rechten.

Dit artikel wordt aangevuld teneinde die taak toe te kennen aan de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R." in het kader van de verwerkingen die ze uitvoeren in de gemeenschappelijke gegevensbank "T.E.R.".

Art. 41

In artikel 149 van de wet gegevensbescherming worden een aantal verplichtingen vastgelegd voor de verwerkingsverantwoordelijke. Zo zorgt hij ervoor dat de toegang tot de persoonsgegevens en de verwerkingsmogelijkheden beperkt blijven tot wat nuttig is in het kader van de doeleinden van de gemeenschappelijke gegevensbank "T.E.R." bedoeld in artikel 5, tweede lid, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.").

Art. 42

Artikel 155 heeft betrekking op het beheer van de inbreuken op de beveiliging. Dat artikel wordt gewijzigd teneinde rekening te houden met de bijzondere regels

dans le cadre de la banque de données commune T.E.R. prévue par le présent projet.

Art. 43

L'article 156 concerne la tenue d'un registre portant sur les banques de données par le responsable du traitement ainsi que sur son contenu. Cette obligation est également d'application dans le cadre de la banque de données commune "T.E.R.".

Art. 44

Cet article reprend l'article 44/11/3^{quinquies}/1, de la loi sur la fonction de police ainsi que l'article 5, alinéas 1^{er} et 2, de l'arrêté royal "TF" et l'arrêté royal "PH". Il concerne la désignation du délégué à la protection des données pour la banque de données commune ainsi que ses missions.

Suite à l'avis du Comité R du 13 juillet 2023 (§ 6) et à l'avis 73.442/2 du 7 juin 2023 du Conseil d'État qui estime que l'ancien article 29, § 3, 4^o, et § 4, paraphrase inutilement l'article 157, § 3, alinéa 2, et § 4, de la loi du 30 juillet 2018 relative à la protection des données, il a été décidé d'introduire un nouvel article 157/1 dans la loi relative à la protection des données. Cet article contient les règles générales de traitement de données liées au délégué à la protection des données mais aussi les spécificités des missions du délégué à la protection des données dans le cadre de la banque de données commune T.E.R. En effet, le délégué à la protection des données doit traiter avec les responsables du traitement conjoints de la banque de données mais également avec le gestionnaire et le responsable opérationnel.

Ainsi, les missions du délégué à la protection des données initialement prévues sont conservées mais davantage développées et renforcées.

Suite à l'avis du Comité R du 13 juillet 2023 (§ 6), la mission de 'mise en œuvre, mise à jour et contrôle d'une politique de sécurisation et de protection des données' a été supprimée. Cette mission est en effet contradictoire avec la mission de conseiller de manière indépendante toute mesures utiles afin d'assurer la sécurité des données enregistrées.

En plus de certains aspects spécifiques de la fonction pour la banque de données commune T.E.R., le régime

pour het beheer van inbreuken op de beveiliging in het kader van de in dit ontwerp bedoelde gemeenschappelijke gegevensbank T.E.R.

Art. 43

Artikel 156 betreft het bijhouden van een register van de gegevensbanken door de verwerkingsverantwoordelijke alsook van de inhoud ervan. Die verplichting is ook van toepassing in het kader van de gemeenschappelijke gegevensbank "T.E.R.".

Art. 44

Dit artikel herneemt artikel 44/11/3^{quinquies}/1 van de wet op het politieambt alsmede artikel 5, eerste en tweede lid, van het koninklijk besluit "TF" en het koninklijk besluit "HP". Het betreft de aanwijzing van de functionaris voor gegevensbescherming voor de gemeenschappelijke gegevensbank alsook zijn opdrachten.

Ingevolge het advies van 13 juli 2023 van Comité I (§ 6) en advies nr. 73.442/2 van 7 juni 2023 van de Raad van State, die van oordeel is dat het oude artikel 29, § 3, 4^o, en § 4, een overbodige parafrase is van artikel 157, § 3, tweede lid, en § 4, van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, werd er besloten een nieuw artikel 157/1 in de voormelde wet in te voegen. Dit artikel bevat de algemene regels voor de gegevensverwerking in samenhang met de functionaris voor de gegevensbescherming, alsook de specifieke kenmerken van de opdrachten van de functionaris voor de gegevensbescherming in het kader van de gemeenschappelijke gegevensbank T.E.R. De functionaris voor gegevensbescherming moet namelijk samen met de gezamenlijke verwerkingsverantwoordelijken alsook met de beheerder en de operationeel verantwoordelijke instaan voor verwerking van de gegevensbank.

De oorspronkelijk voorziene opdrachten van de functionaris voor gegevensbescherming, worden dus behouden maar verder uitgewerkt en aangescherpt.

Ingevolge het advies van 13 juli 2023 van Comité I (§ 6) werd de opdracht van 'het toepassen, het bijwerken en het controleren van een beleid inzake beveiliging en bescherming van gegevens' geschrapt. Die taak lijkt inderdaad in strijd te zijn met de taak om onafhankelijk advies te verlenen over nuttige maatregelen om de beveiliging van geregistreerde gegevens te waarborgen.

Naast bepaalde specifieke aspecten van de functie voor de gemeenschappelijke gegevensbank T.E.R. wordt

applicable au délégué à la protection des données est complété des dispositions de l'article 157 de la loi relative à la protection des données. Les dispositions de la loi sur la fonction de police ne précisaient pas tous les aspects du rôle du délégué à la protection des données, ce qui pouvait déformer son action. Puisque, il a été décidé d'aligner le régime applicable aux traitements des données à caractère personnel sur le régime du sous-titre 4, du titre 3, de la loi relative la protection des données, c'est tout naturellement sur ce sous-titre également que le régime du délégué à la protection des données de la banque de données commune a été aligné.

Le nouvel article 157/1 insiste sur le caractère collaboratif du rôle du délégué à la protection des données pour la banque de données commune T.E.R.: la banque de données commune T.E.R. vit grâce et par la collaboration des services de base et des partenaires de la banque de données commune T.E.R.

Quelques précisions sont dès lors apportées quant à la relation du délégué à la protection des données avec les services traitant de données de la banque de données commune T.E.R.

Ainsi, il veillera, dans le cadre de ses compétences, à sensibiliser les utilisateurs de tous les services. Il épaulera également le gestionnaire dans l'élaboration des procédures de traitement.

Afin de coordonner les missions en matière de sécurité et de protection de la vie privée, le délégué à la protection des données de la banque de données commune T.E.R. pourra aussi être amené à collaborer avec les experts travaillant dans les services traitant des données de la banque de données commune T.E.R.

Cette collaboration avec les responsables quotidiens et les autres partenaires de la banque de données commune T.E.R. est primordiale afin que le délégué à la protection des données puisse, en connaissance de cause, exercer en toute indépendance sa mission de contrôle, mais en veillant aussi à respecter les compétences de chacun.

Enfin, le délégué à la protection des données fait également office de point de contact avec les autorités de contrôle compétentes sur les questions relatives aux traitements réalisés dans la banque de données commune T.E.R.

À noter que le principe de l'indépendance du délégué à la protection des données visé à l'article 5, alinéa 3,

de la loi relative à la protection des données est complété des dispositions de l'article 157 de la loi relative à la protection des données. Les dispositions de la loi sur la fonction de police ne précisaient pas tous les aspects du rôle du délégué à la protection des données, ce qui pouvait déformer son action. Puisque, il a été décidé d'aligner le régime applicable aux traitements des données à caractère personnel sur le régime du sous-titre 4, du titre 3, de la loi relative la protection des données, c'est tout naturellement sur ce sous-titre également que le régime du délégué à la protection des données de la banque de données commune a été aligné.

Het nieuw artikel 157/1 wijst nadrukkelijk op de samenwerking die de rol van de functionaris voor gegevensbescherming voor de gemeenschappelijke gegevensbank T.E.R. behelst: de gemeenschappelijke gegevensbank T.E.R. bestaat dankzij de samenwerking van de basisdiensten en de partners van de gemeenschappelijke gegevensbank T.E.R.

Daarom worden enkele verduidelijkingen aangebracht wat betreft de relatie van de functionaris voor gegevensbescherming met de diensten die de gegevens uit de gemeenschappelijke gegevensbank T.E.R. verwerken.

Aldus waakt hij erover, in het raam van zijn bevoegdheden, om de gebruikers van alle diensten te sensibiliseren. Hij zal eveneens de beheerder bijstaan bij het uitwerken van verwerkingsprocedures.

Ten slotte, teneinde de opdrachten inzake veiligheid en bescherming van de persoonlijke levenssfeer te coördineren, kan de functionaris voor gegevensbescherming van de gemeenschappelijke gegevensbank T.E.R. ertoe gebracht worden samen te werken met de experts van diensten die gegevens verwerken van de gemeenschappelijke gegevensbank T.E.R.

Deze samenwerking met de dagelijkse verantwoordelijken en de overige partners van de gemeenschappelijke gegevensbank T.E.R. is van primordiaal belang de functionaris voor gegevensbescherming, met kennis van zaken, zijn controleopdracht in alle onafhankelijkheid kan uitoefenen, maar er tevens voor kan zorgen dat de bevoegdheden van elkeen worden gerespecteerd.

Ten slotte fungeert de functionaris voor gegevensbescherming ook als contactpunt met de bevoegde toezichthoudende autoriteiten over aangelegenheden in verband met de verwerkingen die in de gemeenschappelijke T.E.R.-gegevensbank worden uitgevoerd.

Opgemerkt dient te worden dat het principe van de onafhankelijkheid van de functionaris voor

de l'arrêté royal "TF" et l'arrêté royal "PH" est repris au paragraphe 5.

Afin de faciliter les missions du délégué à la protection des données, l'article 157/1 veille à ce qu'il soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel par le responsable du traitement visé à l'article 5, alinéa 1^{er}, le gestionnaire et le responsable opérationnel et à ce qu'il dispose des ressources nécessaires lui permettant d'exercer ses missions. Il pourra également être assisté par un ou plusieurs adjoints.

Art. 45

L'article 158 de la loi relative à la protection des données dispose qu'une consultation du délégué à la protection des données ou de l'autorité de contrôle compétente ou une analyse d'impact ne peuvent pas être exigées comme préalable à la transmission des informations entre l'OCAM et tout organisme public ou privé dans l'intérêt de l'exercice des missions de l'OCAM.

Dans l'intérêt de l'exercice des missions de prévention et de suivi du terrorisme et de l'extrémisme, lorsqu'il peut mener au terrorisme, visées à l'article 3, alinéa 1^{er}, de la loi du xx portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R."), la même exception est prévue pour la communication de données à caractère personnel issues de la banque de données commune "T.E.R." à tout organisme public ou privé.

Art. 46

Dans l'article 161 de la loi relative à la protection des données, l'Organe de contrôle de l'information policière, et le Comité permanent de contrôle des services de renseignement et de sécurité sont désignées conjointement comme autorités de protection des données chargées du contrôle du traitement des données à caractère personnel dans la banque de données commune "T.E.R."

Art. 47

Plus particulièrement au sujet de l'article 47, il faut mentionner que l'utilisation de données contenues dans la banque de données commune T.E.R. à des fins historiques, scientifiques ou statistiques devra faire l'objet d'un protocole entre le responsable opérationnel et le service destinataire. Le protocole déterminera notamment

gegevensbescherming bedoeld in artikel 5, derde lid, van het koninklijk besluit "TF" en het koninklijk besluit "HP", wordt hernomen in paragraaf 5.

Om de opdrachten van de functionaris voor gegevensbescherming te vergemakkelijken, ziet het artikel 157/1 erop toe dat deze op passende wijze en te zijner tijd bij alle aangelegenheden betreffende de bescherming van persoonsgegevens betrokken wordt door de verwerkingsverantwoordelijke bedoeld in artikel 5, eerste lid, de beheerder en de operationeel verantwoordelijke, en dat deze beschikt over de nodige middelen voor het vervullen van zijn opdrachten. Hij kan ook worden bijgestaan door een of meer adjuncten.

Art. 45

Artikel 158 van de wet gegevensbescherming bepaalt dat een raadpleging van de functionaris voor gegevensbescherming of de bevoegde toezichhoudende autoriteit of een impactanalyse geen voorafgaande vereiste kunnen zijn voor de mededeling van informatie tussen het OCAD en enig openbaar of particulier orgaan, in het belang van de uitvoering van de opdrachten van het OCAD.

In het belang van de uitvoering van de opdrachten inzake de voorkoming en de opvolging van terrorisme en extremisme, dat kan leiden tot terrorisme, bedoeld in artikel 3, eerste lid, van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R."), geldt dezelfde uitzondering voor de mededeling van persoonsgegevens van de gemeenschappelijke gegevensbank "T.E.R." aan enig openbaar of particulier orgaan.

Art. 46

In artikel 161 van de wet gegevensbescherming worden het Controleorgaan op de politieke informatie, en het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten gezamenlijk aangewezen als gegevensbeschermingsautoriteiten belast met de controle van de verwerking van persoonsgegevens in de gemeenschappelijke gegevensbank "T.E.R."

Art. 47

Meer bepaald met betrekking tot artikel 47 dient te worden vermeld dat het gebruik van gegevens uit de gemeenschappelijke gegevensbank T.E.R. voor historische, wetenschappelijke of statistische doeleinden moet worden vastgelegd in een protocol tussen de operationeel verantwoordelijke en de dienst-bestemming.

les données nécessaires pour réaliser la recherche et si les données doivent être anonymisées.

Suite à l'avis 73.442/2 le Conseil d'État du 7 juin 2023 et du Comité R du 13 juillet 2023 (§ 4), la dérogation apportée à l'article 162, alinéa 1^{er}, de la loi précitée est complétée. Elle prévoit ainsi une réserve à l'autorisation de consultation à des fins historiques, scientifiques ou statistiques dans l'hypothèse où cette dernière peut nuire à la sécurité d'une personne, à l'exercice de l'action publique, à l'exercice d'une enquête de renseignement, ou à la relation avec un service répressif d'un État étranger ou avec un service de renseignement et de sécurité d'un État étranger. Cette réserve est d'ailleurs également prévue par l'article 19 de l'avant-projet.

Cet article prévoit également que "Toute demande adressée aux Archives de l'État de traitement ultérieur de données à caractère personnel enregistrées dans la banque de données commune "T.E.R." à d'autres fins que celles visées à l'alinéa 3 est refusée à moins que la finalité soit légitime". Le terme "finalité légitime" n'est pas neuf. En effet, cet alinéa est formulé de la même façon à l'alinéa 2 de l'article 162 actuel, ainsi qu'à l'article 99, al. 2, de la loi relative à la protection des données pour les services de renseignement. Le caractère légitime s'apprécie sur le fondement juridique de la demande. Les critères sont fixés dans les dispositions qui suivent dans le chapitre X du sous-titre 4, Titre 3, de la loi relative à la protection des données. Par exemple, l'article 164 prévoit que si la finalité historique ne peut être obtenue avec des informations pseudonymisées, l'OCAM peut autoriser la consultation des info "claires" s'il n'y a pas une atteinte disproportionnée à la vie privée (c'est donc un critère qui permet d'apprécier la légitimité de la demande). Par ailleurs, les travaux parlementaires de la loi du 30 juillet 2018 relative à la protection des données précise au sujet de l'article 99, al.2, que "Pour répondre à l'avis du Conseil d'État, en page 35, l'alinéa 2 de cet article est reformulé: il est précisé qu'un traitement ultérieur sans finalités historiques, statistiques ou scientifiques est refusé sauf si la finalité est légitime et que la consultation n'est pas susceptible de porter aux intérêts à protéger qui sont visés à l'alinéa premier. Ainsi, il est clair qu'il n'est pas question d'autoriser une finalité – celle-ci devant en elle-même et au préalable être légitime – mais bien une consultation de données dans certains cas. Les critères étant déterminés, il ne s'agit pas d'un pouvoir discrétionnaire. Les modalités sont celles fixées dans le

Het protocol zal met name de noodzakelijke gegevens bepalen voor de uitvoering van het onderzoek, en of de gegevens moeten worden geanonimiseerd.

Ingevolge advies nr. 73.442/2 van 7 juni 2023 van de Raad van State en het advies van 13 juli 2023 van Comité I (§ 4) wordt de aan artikel 162, eerste lid, van de voornoemde wet aangebrachte afwijking, aangevuld. Zo wordt er voorzien in enig voorbehoud voor de toestemming tot raadpleging voor historische, wetenschappelijke of statistische doeleinden in zoverre die raadpleging de veiligheid van een persoon, de uitoefening van de strafvordering, de uitoefening van een inlichtingenonderzoek of de relatie met een rechtshandavingsinstantie van een buitenlandse Staat of met een inlichtingen- en veiligheidsdienst van een buitenlandse Staat in het gedrang kan brengen. Dat voorbehoud wordt overigens eveneens opgenomen in artikel 19 van het voorontwerp.

Dit artikel bepaalt ook dat "Elke vraag aan de Rijksarchieven om verdere verwerking van persoonsgegevens geregistreerd in de gemeenschappelijke gegevensbank "T.E.R." voor overige doelen dan die bedoeld in het derde lid wordt geweigerd tenzij het doel, legitiem is". De uitdrukking "legitiem doel" is niet nieuw. Dit lid is immers geformuleerd op dezelfde wijze als huidige artikel 192, tweede lid en als artikel 99, tweede lid van de wet betreffende de gegevensbescherming voor de inlichtingendiensten. Het legitieme karakter wordt beoordeeld aan de hand van de juridische gegrondheid van de vraag. De criteria zijn vastgelegd in de bepalingen die volgen in hoofdstuk X van subtitel 4, Titel 3, van de wet betreffende de gegevensbescherming. Zo bijvoorbeeld bepaalt artikel 164 dat, indien gepseudonimiseerde gegevens niet toelaten om de historische doeleinden te verwezenlijken, het OCAD de raadpleging van "clear" info kan toestaan indien dit geen onevenredige afbreuk doet aan het privéleven (het betreft dus een criterium waarmee de legitimiteit van de vraag kan worden beoordeeld). Voorts wordt in het kader van de parlementaire voorbereidingen voor de wet van 30 juli 2018 betreffende de bescherming van de persoonsgegevens in verband met artikel 99, tweede lid, bepaald: "Om te antwoorden op het advies van de Raad van State (pagina 35) wordt het tweede lid van dit artikel opnieuw geformuleerd: er wordt verduidelijkt dat een verdere verwerking zonder historische, statistische of wetenschappelijke doeleinden geweigerd wordt behalve indien het doeleinde wettelijk is en de raadpleging geen afbreuk kan doen aan de belangen bedoeld in het eerste lid. Zo moet het duidelijk zijn dat er geen sprake is van het toelaten van een doeleinde – deze dient op zich en voorafgaand wettelijk

présent chapitre et, le cas échéant, dans d'autres lois (par exemple la loi du 11 décembre 1998).".

À noter que l'alinéa 2 du nouvel article 162 a été complété conformément à l'avis du Conseil d'État 73.442/2 du 7 juin 2023.

Art. 48

L'article 164 de la loi relative à la protection des données concerne l'anonymisation ou la pseudonymisation des données dans le cadre de la consultation à des fins historiques, scientifiques ou statistiques des données à caractère personnel de l'OCAM et de son personnel par un responsable du traitement ultérieur.

Le même principe est prévu pour le traitement ultérieur de données contenues dans la banque de données commune T.E.R. à des fins historiques, scientifiques ou statistiques. Le responsable opérationnel, à savoir l'OCAM, doit se concerter avec les services de base visé à l'article 2, 2°, de la loi du xxx portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.").

Art. 49

L'article 165 de la loi relative à la protection des données prévoit que toute communication et toute publication des données consultées non anonymisées et non pseudonymisées ne peuvent avoir lieu qu'avec l'autorisation de l'OCAM.

Ici aussi, le même principe s'applique pour la banque de données commune T.E.R. Toute communication et toute publication des données consultées non anonymisées et non pseudonymisées ne peuvent avoir lieu qu'avec l'autorisation du responsable opérationnel (OCAM) après concertation avec les services de base visé à l'article 2, 2°, de la loi du xxx portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.").

Art. 50

L'article 166 de la loi relative à la protection des données impose la tenue d'un journal du traitement ultérieur par le responsable du traitement.

te zijn – maar wel een raadpleging van gegevens in bepaalde gevallen. Aangezien de criteria vastliggen betreft het geen zins een discretionaire bevoegdheid. De modaliteiten zijn deze die zijn vastgelegd in huidige hoofdstuk en, desgevallend, in andere wetten (bijvoorbeeld de wet van 11 december 1998).".

Het tweede lid van het nieuwe artikel 162 is aangevuld overeenkomstig advies 73.442/2 van de Raad van State van 7 juni 2023.

Art. 48

Artikel 164 van de wet gegevensbescherming betreft de anonimisering of pseudonimisering van gegevens in het kader van de raadpleging voor historische, wetenschappelijke of statistische doeleinden van persoonsgegevens van het OCAD en zijn personeelsleden door een verdere verwerkingsverantwoordelijke.

Er wordt in hetzelfde principe voorzien voor de verdere verwerking van gegevens in de gemeenschappelijke gegevensbank T.E.R. voor historische, wetenschappelijke of statistische doeleinden. De operationeel verantwoordelijke, met andere woorden het OCAD, moet overleg plegen met de basisdiensten bedoeld in artikel 2, 2° van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.").

Art. 49

Artikel 165 van de wet gegevensbescherming bepaalt dat enige mededeling of publicatie van geraadpleegde niet-geanonimiseerde of niet-gepseudonimiseerde gegevens enkel mogelijk is met het akkoord van het OCAD.

Dat principe geldt hier ook voor de gemeenschappelijke gegevensbank T.E.R. Enige mededeling of publicatie van geraadpleegde niet-geanonimiseerde of niet-gepseudonimiseerde gegevens is enkel mogelijk met het akkoord van de operationeel verantwoordelijke (het OCAD) na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.").

Art. 50

Artikel 166 van de wet gegevensbescherming legt de verwerkingsverantwoordelijke op een logbestand betreffende de verdere verwerking te bewaren.

Il en sera de même pour la banque de données commune "T.E.R.".

Section 2

Disposition modificative de la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme

Art. 51

Cet article apporte des corrections de renvoi dans l'article 4 de la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme.

Section 3

Dispositions modificatives de la loi du 5 août 1992 sur la fonction de police

Art. 52

Cette disposition vise à optimiser la coopération entre les différents services (services de police, services d'urgence et de secours et services de la santé) qui doivent intervenir en réponse à des incidents mineurs ou majeurs et, en particulier, à garantir l'intégrité physique et psychologique de la personne concernée elle-même et de toute personne susceptible d'entrer en contact avec elle dans le cadre de l'intervention des services précités.

Comme précisé précédemment, contrairement à ce que recommande le C.O.C. dans son avis du 20 juin 2023, il est préférable de ne pas prévoir une communication nécessairement écrite de ces informations. En effet, cette disposition entend s'appliquer à des situations d'urgence qui nécessitent dès lors une communication orale. Par ailleurs, une communication écrite de ces informations au prestataire de soin peut entraîner un problème de sécurité. Néanmoins, cette communication à l'égard d'un prestataire de soin devra faire l'objet de précision dans une circulaire ministérielle.

Dat geldt ook voor de gemeenschappelijke gegevensbank "T.E.R.".

Afdeling 2

Wijzigingsbepaling van de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme

Art. 51

Dit artikel corrigeert de verwijzingen in artikel 4 van de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme.

Afdeling 3

Wijzigingsbepaling van de wet van 5 augustus 1992 op het politieambt

Art. 52

De bepaling strekt ertoe om de samenwerking tussen verschillende diensten (politiediensten, hulp en reddingsdiensten en gezondheidsdiensten) die naar aanleiding van kleine of grote incidenten moeten tussenkomen te optimaliseren en in het bijzonder om de fysieke en psychische integriteit te waarborgen van de betrokken persoon zelf en eenieder die in contact kan komen met de betrokken persoon in het kader van het optreden de voornoemde diensten.

Zoals hierboven verduidelijkt, verdient het, in tegenstelling van wat het COC aanbeveelt in zijn advies van 20 juni 2023, de voorkeur niet te bepalen dat die communicatie van de informatie noodzakelijkerwijs schriftelijk dient te gebeuren. Deze bepaling is immers tevens van toepassing op spoedeisende situaties waarvoor derhalve mondeling moet worden gecommuniceerd. Bovendien kan het schriftelijk communiceren van dergelijke informatie aan de zorgverlener aanleiding geven tot een veiligheidsprobleem. Niettemin moet deze communicatie ten aanzien van een zorgverlener nader worden verduidelijkt in een ministeriële omzendbrief.

Section 4*Dispositions modificatives du Code consulaire***Art. 53 et 54**

Ces articles apportent des corrections de renvoi dans les articles 39/4 et 65/1 du Code consulaire.

CHAPITRE 5**Dispositions abrogatoires****Art. 55**

Cet article abroge les dispositions actuelles de la loi sur la fonction de police relative à la banque de données TF et PH, à savoir les articles 44/2, § 2, 44/4, § 2, dernier alinéa et 44/11/3bis à 44/11/3quinquies/2.

Dans son avis du 13 juillet 2023, le Comité R s'interroge sur la transition des banques de données "TF" et "PH" à la banque de données commune T.E.R. (§ 39). Il faut rappeler ici qu'il n'est pas question d'un transfert de données mais seulement d'un changement de base légale de la banque de données existante. Par ailleurs, comme déjà expliqué, dans les faits, il existe actuellement une seule banque de données et non pas deux banques de données "TF" et "PH".

Art. 56 et 57

Conformément à l'avis 73.442/2 du Conseil d'État du 7 juin 2023, "En raison de la conception d'un nouveau texte législatif autonome rassemblant des dispositions légales et réglementaires existantes, il convient de prévoir que les dispositions qui sont issues des arrêtés royaux du 21 juillet 2016 "relatif à la banque de données communes *Terrorist Fighters*" 14 et du 23 avril 2018 "relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1^{re} bis "de la gestion des informations" du chapitre IV de la loi sur la fonction de police" seront abrogées à la même date que la date d'entrée en vigueur de l'avant-projet."

Afdeling 4*Wijzigingsbepalingen van de Consulaire Wetboek***Art. 53 et 54**

Deze artikelen corrigeren de verwijzingen in de artikelen 39/4 en 65/1 van de consulaire code.

HOOFDSTUK 5**Opheffingsbepalingen****Art. 55**

Bij dit artikel worden de huidige bepalingen van de wet op het politieambt met betrekking tot de gegevensbank TF en PH ingetrokken, namelijk de artikelen 44/2, § 2, 44/4, § 2, laatste lid en 44/11/3bis tot en met 44/11/3quinquies/2.

In het advies van 13 juli 2023 heeft Comité I vragen bij de overdracht van gegevensbanken "TF" en "HP" naar de gemeenschappelijke gegevensbank T.E.R. (§ 39). Hier moet worden gewezen op het feit dat er geen sprake is van een overdracht van gegevens, maar louter een verandering van de wettelijke grondslag voor de bestaande gegevensbank. Bovendien bestaat er, zoals reeds uitgelegd, thans in feite één gegevensbank en niet twee gegevensbanken "TF" en "HP".

Art. 56 en 57

In advies nr. 73.442/2 van 7 juni 2023 stelt de Raad van State het volgende: "Aangezien een nieuwe op zichzelf staande wetgevende tekst wordt ontworpen die bestaande wettelijke en verordenende bepalingen samenbrengt, dient te worden voorzien dat de bepalingen die afkomstig zijn van het koninklijk besluit van 21 juli 2016 "betreffende de gemeenschappelijke gegevensbank *Terrorist Fighters*" 14 en van het koninklijk besluit van 23 april 2018 "betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1bis "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt" worden opgeheven op dezelfde datum als de datum van inwerkingtreding van het voorontwerp."

CHAPITRE 6

Dispositions finales

Art. 58

Cet article donne une habilitation au Roi pour modifier les textes législatifs ou réglementaires existants qui font référence soit aux dispositions de la loi sur la fonction de police (alinéa 1^{er}), soit aux dispositions de l'AR "TF" et l'AR "PH" (alinéa 2) par les nouvelles dispositions correspondantes de la loi ou de ses arrêtés d'exécution.

L'avis 73.442/2 du Conseil d'État du 7 juin 2023 a été suivi sur ce point à l'exception de l'abrogation de l'alinéa 1^{er}. Si cette habilitation est supprimée, il ne sera pas possible pour le Roi de remplacer, dans les lois et arrêtés royaux, les références existantes aux dispositions de la loi sur la fonction de police par les références aux dispositions correspondantes de la présente loi ou de ses arrêtés d'exécution.

Art. 59

Cet article prévoit une mesure transitoire pour les entités qui sont enregistrées dans une banque de données commune visée à l'article 44/2, § 2, de la loi sur la fonction de police, au moment de l'entrée en vigueur de la présente loi. Ainsi, pour les entités qui sont enregistrées dans la banque de données commune actuelle, la TFL procèdera à la concertation mise en place par l'article 32, § 1^{er}, lorsque de nouvelles données à caractère personnel et informations visées à l'article 31 peuvent entraîner un changement de mesures à l'égard de ladite entité.

Art. 60

Cet article prévoit que le Roi peut fixer la date d'entrer en vigueur de la présente loi à une date antérieure que le 1^{er} janvier 2025. Pour éviter tout vide juridique, il est important que la loi entre en vigueur lorsque l'arrêté royal portant exécution de la présente loi sera prêt.

HOOFDSTUK 6

Slotbepalingen

Art. 58

Dit artikel verleent de Koning een machtiging om in bestaande wetgevende of regelgevende teksten de verwijzingen naar ofwel bepalingen van de wet op het politieambt (eerste lid), ofwel bepalingen van het KB "TF" en het KB "HP" (tweede lid) te wijzigen in verwijzingen naar de nieuwe ermee overeenstemmende bepalingen van de wet of van haar uitvoeringsbesluiten.

Advies nr. 73.442/2 van 7 juni 2023 van de Raad van State werd voor dat punt gevolgd, behoudens de weglating van het eerste lid. Indien deze machtiging wordt weggelaten, zal de Koning de bestaande verwijzingen in wetten en koninklijke besluiten naar bepalingen van de wet op het politieambt niet kunnen vervangen door verwijzingen naar de ermee overeenstemmende bepalingen van deze wet of van haar uitvoeringsbesluiten.

Art. 59

In dit artikel wordt voorzien in een overgangsbepaling voor de entiteiten die in de gemeenschappelijke gegevensbank bedoeld in artikel 44/2, § 2, van de wet op het politieambt zijn opgenomen op het ogenblik van de inwerkingtreding van deze wet. Aldus gaat de LTF, voor de entiteiten die in de huidige gemeenschappelijke gegevensbank zijn opgenomen, over tot het bij artikel 33, § 1, ingevoerd overleg wanneer nieuwe persoonsgegevens en informatie zoals bedoeld in artikel 30 kunnen leiden tot een verandering van maatregelen ten aanzien van deze entiteit.

Art. 60

Dit artikel bepaalt dat de Koning de datum van inwerkingtreding van deze wet kan vaststellen op een eerdere datum dan 1 januari 2025. Teneinde iedere juridische lacune te voorkomen, is het belangrijk dat de wet in werking treedt wanneer het koninklijk besluit tot uitvoering van deze wet klaar is.

Le but est que le projet de loi et d'arrêté royal entrent en vigueur encore sous cette législature. Nous proposons dès lors de prendre une date ultime (et au plus tard) le 1^{er} janvier 2025.

Le ministre de la Justice,

Paul Van Tigchelt

La ministre de l'Intérieur,

Annelies Verlinden

Het is de bedoeling dat de ontwerpen van wet en van koninklijk besluit nog binnen deze regeerperiode in werking treden. Derhalve stellen we als (uiterste) deadline 1 januari 2025 voor.

De minister van Justitie,

Paul Van Tigchelt

De minister van Binnenlandse Zaken,

Annelies Verlinden

AVANT-PROJET DE LOI

soumis à l'avis du Conseil d'État

Avant-projet de loi portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police

Chapitre 1^{er} – Dispositions générales

Article 1^{er}. La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2. Pour l'application de la présente loi et de ses arrêtés d'exécution, il faut entendre par:

1° "loi relative à la protection des données": la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel;

2° "services de base": l'Organe de la coordination pour l'analyse de la menace, la police intégrée et les services de renseignement et de sécurité;

3° "services partenaires":

a) les unités opérationnelles du Centre de Crise national du Service Public fédéral Intérieur;

b) la Direction Générale Sécurité et Prévention du Service Public fédéral Intérieur;

c) la Direction Générale des Etablissements Pénitentiaires du Service Public fédéral Justice;

d) la Direction générale Affaires Consulaires du Service Public fédéral Affaires étrangères;

e) le Ministère public;

f) la Cellule de Traitement des Informations Financières;

g) la Direction générale de l'Office des Etrangers du Service Public fédéral Intérieur;

h) l'Administration générale des douanes et accises du Service Public fédéral Finances;

i) le service des cultes et de la laïcité du Service Public fédéral Justice;

j) l'Administration générale de la Trésorerie du Service Public fédéral Finances;

VOORONTWERP VAN WET

onderworpen aan het advies van de Raad van State

Voorontwerp van wet tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.") en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt

Hoofdstuk 1 – Algemene bepalingen

Artikel 1. Deze wet regelt een aangelegenheid zoals bedoeld in artikel 74 van de Grondwet.

Art. 2. Voor de toepassing van deze wet en de uitvoeringsbesluiten ervan wordt verstaan onder:

1° "wet gegevensbescherming": de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens;

2° "basisdiensten": het Coördinatieorgaan voor de dreigingsanalyse, de geïntegreerde politie, de inlichtingen- en veiligheidsdiensten;

3° "partnerdiensten":

a) de operationele eenheden van de Nationaal Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken;

b) de Algemene Directie Veiligheid en Preventie van de Federale Overheidsdienst Binnenlandse Zaken;

c) het Directoraat-generaal Penitentiaire Inrichtingen van de Federale Overheidsdienst Justitie;

d) het Directoraat-generaal Consulaire Zaken van de Federale Overheidsdienst Buitenlandse Zaken;

e) het Openbaar Ministerie;

f) de Cel voor Financiële Informatieverwerking;

g) de Algemene Directie Dienst Vreemdelingenzaken van de Federale Overheidsdienst Binnenlandse Zaken;

h) de Algemene Administratie van de douane en accijnzen van de Federale Overheidsdienst Financiën;

i) de dienst Erediensten en Vrijzinnigheid van de Federale Overheidsdienst Justitie;

j) de Algemene administratie van de Thesaurie van de Federale Overheidsdienst Financiën;

k) dans le cadre de leurs missions légales d'accompagnement judiciaire et de la surveillance d'auteurs d'infractions, l'Administration générale des Maisons de Justice de la Communauté Française, le département Maison de Justice du Ministère de la Communauté Germanophone, l'Agence flamande pour la Justice et le Maintien, l'Administration générale de l'Aide à la Jeunesse de la Communauté Française, le service d'Aide à la Jeunesse de la Communauté germanophone et l'Agence flamande Opgroeien;

4° "entité": toute personne physique majeure ou mineure de plus de douze ans ou toute personne morale, association de fait, ainsi que l'ensemble des moyens utilisés, déterminés par le Roi en application de l'article 6, § 2, alinéa 4;

5° "données à caractère personnel": les données à caractère personnel au sens de l'article 4, 1), du Règlement Général sur la protection des données et de l'article 26, 1°, de la loi relative à la protection des données qui sont non classifiées conformément à la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

6° "informations": informations non classifiées conformément à la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité que les services de base et les services partenaires traitent dans le cadre de leurs missions légales respectives;

7° "banque de données commune T.E.R.": la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" visée à l'article 3;

8° "évaluation de la menace": évaluation, au sens de l'article 8, alinéa 1^{er}, 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace, pour les entités reprises dans la banque de données commune T.E.R.

9° "fiche de renseignements": fiche qui contient l'ensemble des données à caractère personnel et des informations relatives à une entité de la banque de données commune T.E.R. provenant de l'ensemble des services qui l'alimentent;

10° "carte d'information": fiche d'une entité qui consiste en un extrait de la fiche de renseignements, contenant les données à caractère personnel et informations, strictement limitées au besoin d'en connaître du destinataire, pour le suivi des entités;

11° "droit de création": l'enregistrement d'une nouvelle entité dans la banque de données commune T.E.R.;

12° "droit de lecture": la consultation de l'ensemble des données à caractère personnel et des informations de la banque de données commune T.E.R.;

13° "droit d'écriture": l'introduction, modification ou effacement des données à caractère personnel et des informations dans la banque de données commune T.E.R.;

k) In het kader van hun wettelijke opdrachten van justitiële begeleiding van en toezicht op daders van misdrijven, de Algemene Administratie van Justitiehuisen van de Franse Gemeenschap, het departement Justitiehuis van het Ministerie van de Duitstalige gemeenschap, het Vlaams Agentschap Justitie en Handhaving, de Algemene Administratie van de hulpverlening aan de jeugd van de Franse Gemeenschap, de dienst voor de hulpverlening aan de jeugd van de Duitstalige gemeenschap en het Vlaams Agentschap Opgroeien;

4° "entiteit": elke meerderjarige natuurlijke persoon of minderjarige natuurlijke persoon ouder dan twaalf jaar of elke rechtspersoon, feitelijke vereniging alsook alle aangewende middelen, bepaald door de Koning, met toepassing van artikel 6, § 2, vierde lid;

5° "persoonsgegevens": persoonsgegevens overeenkomstig artikel 4, 1), van de Algemene Verordening Gegevensbescherming en artikel 26, 1° van de wet gegevensbescherming die niet geclassificeerd zijn overeenkomstig de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

6° "informatie": niet-geclassificeerde informatie overeenkomstig de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen die de basisdiensten en de partnerdiensten verwerken in het kader van hun respectievelijke wettelijke opdrachten;

7° "gemeenschappelijke gegevensbank T.E.R.": de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" bedoeld in artikel 3;

8° "dreigingsevaluatie": evaluatie in de zin van artikel 8, eerste lid, 2°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging voor de entiteiten die zijn opgenomen in de gemeenschappelijke gegevensbank T.E.R.;

9° "inlichtingenfiche": fiche die alle persoonsgegevens en informatie met betrekking tot een entiteit van de gemeenschappelijke gegevensbank T.E.R. bevat die afkomstig zijn van alle diensten die haar voeden;

10° "informatiekaart": fiche van een entiteit die een uittreksel van de inlichtingenfiche vormt, en die de persoonsgegevens en informatie bevat die strikt beperkt zijn tot de behoefte om te kennen van de bestemming, voor de opvolging van de entiteiten;

11° "creatierecht": de opname van een nieuwe entiteit in de gemeenschappelijke gegevensbank T.E.R.;

12° "leesrecht": de raadpleging van alle persoonsgegevens en informatie in de gemeenschappelijke gegevensbank T.E.R.;

13° "schrijfrecht": de invoering, wijziging of uitwissing van de persoonsgegevens en informatie in de gemeenschappelijke gegevensbank T.E.R.;

14° “droit d’interrogation”: prise de connaissance de l’existence d’une entité dans la banque de données commune T.E.R. et en cas de confirmation de l’existence d’une entité dans la banque de données commune T.E.R., la prise de connaissance de l’évaluation de la menace;

15° “autorités de contrôle”: l’Organe de contrôle de l’information policière, visé à l’article 71 de la loi relative à la protection des données et le Comité permanent de contrôle des services de renseignement et de sécurité, visé à l’article 1^{er} de la loi organique du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l’Organe de coordination pour l’analyse de la menace;

16° “interconnexion”: traitement, au moyen de procédés automatisés, par lequel

a) les données à caractère personnel et les informations de la banque de données commune T.E.R. sont mises en relation avec des données à caractère personnel et informations pertinentes enregistrées dans d’autres banques de données gérées par les services de base ou les services partenaires;

b) les données à caractère personnel et les informations pertinentes des banques de données, sources authentiques peuvent être transférées vers la banque de données commune T.E.R.

Chapitre 2. - De la banque de données commune T.E.R.

Section 1 – Dispositions générales

Art. 3. Il est créé une banque de données commune “Terrorisme, Extrémisme, processus de Radicalisation” qui permet le traitement commun, par tout ou partie des services de base et des services partenaires, des données à caractère personnel et des informations relatives aux missions de prévention et de suivi du terrorisme et de l’extrémisme, lorsqu’il peut mener au terrorisme, au sens de l’article 8, 1°, b) et c) de la loi du 30 novembre 1998 des services de renseignement et de sécurité, de ces services, chacun dans le cadre de ses compétences légales.

La banque de données commune T.E.R. répond à la nécessité de structurer l’ensemble des données à caractère personnel et des informations relatives aux missions visées à l’alinéa premier fournies par les services de base et les services partenaires de sorte qu’elles soient retrouvées directement afin d’accomplir les finalités visées à l’article 5, alinéa 2.

Une organisation dont l’objet réel est exclusivement d’ordre politique, syndical, philanthropique, philosophique ou religieux ou qui poursuit exclusivement tout autre but légitime ne peut, en tant que telle, être reprise dans la banque de données commune T.E.R.

Art. 4. Sans préjudice des articles 11 et 45 de la loi relative à la protection des données, les règles relatives à la protection

14° “vraagrecht”: kennisneming van het bestaan van een entiteit in de gemeenschappelijke gegevensbank T.E.R. en, in geval van bevestiging van het bestaan van een entiteit in de gemeenschappelijke gegevensbank T.E.R., kennisneming van de dreigingsevaluatie;

15° “toezichhoudende overheden”: het Controleorgaan op de politieke informatie, bedoeld in artikel 71 van de wet gegevensbescherming, en het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, bedoeld in artikel 1 van de organieke wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;

16° “koppeling”: de verwerking, via geautomatiseerde procedures, waarbij

a) de persoonsgegevens en informatie van de gemeenschappelijke gegevensbank T.E.R. verbonden worden met persoonsgegevens en relevante informatie die geregistreerd zijn in andere gegevensbanken die door de basisdiensten of de partnerdiensten worden beheerd;

b) de persoonsgegevens en de relevante informatie van de gegevensbanken, authentieke bronnen, kunnen worden overgezonden aan de gemeenschappelijke gegevensbank T.E.R.

Hoofdstuk 2 - De gemeenschappelijke gegevensbank T.E.R.

Afdeling 1 – Algemene bepalingen

Art. 3. Er wordt een gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” gecreëerd die de gemeenschappelijke verwerking mogelijk maakt, door alle of een deel van de basisdiensten en de partnerdiensten, van de persoonsgegevens en informatie betreffende de opdrachten inzake de voorkoming en de opvolging van terrorisme en extremisme, dat kan leiden tot terrorisme, in de zin van artikel 8, 1°, b) en c) van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, van die diensten, elk in het kader van zijn wettelijke bevoegdheden.

De gemeenschappelijke gegevensbank T.E.R. beantwoordt aan de noodzaak tot het structureren van alle persoonsgegevens en informatie betreffende de opdrachten bedoeld in het eerste lid, die aangeleverd worden door de basisdiensten en de partnerdiensten, zodat zij direct worden teruggevonden teneinde de doeleinden bedoeld in artikel 5, tweede lid, te bereiken.

Een organisatie waarvan het feitelijk oogmerk uitsluitend politiek, vakorganisatorisch, menslievend, levensbeschouwelijk of godsdienstig is of die uitsluitend enig ander rechtmatig oogmerk nastreeft, kan als zodanig niet in de gemeenschappelijke gegevensbank T.E.R. worden opgenomen.

Art. 4. Onverminderd artikelen 11 en 45 van de wet gegevensbescherming, zijn de regels inzake gegevensbescherming

des données et aux droits de la personne concernée sont celles visées au Titre 3, sous-titre 4, de la même loi.

Par dérogation à l'article 162 de la loi relative à la protection des données, la consultation des données à caractère personnel et des informations enregistrées dans la banque de données commune T.E.R. pour un traitement ultérieur à des fins historiques, scientifiques ou statistiques est autorisée par le responsable opérationnel après concertation avec les services de base.

Section 2 – Responsables du traitement et finalités

Art. 5. Les ministres de l'Intérieur et de la Justice sont conjointement responsables du traitement de la banque de données commune T.E.R.

Les finalités de la banque de données commune T.E.R. sont les suivantes:

1° la concertation coordonnée entre les services de base et les services partenaires;

2° la nécessité stratégique, tactique ou opérationnelle de traiter en commun des données à caractère personnel et des informations pour exercer les missions respectives des services de base et des services partenaires;

3° l'aide à la prise de décisions par les autorités administratives ou à la prise de décisions de police administrative ou judiciaire;

4° l'analyse, l'évaluation et le suivi, en ce compris la prise de mesures, des entités enregistrées dans la banque de données commune T.E.R. et l'analyse, l'évaluation et le suivi du phénomène du terrorisme et de l'extrémisme lorsqu'il peut mener au terrorisme sur base d'une évaluation de la menace.

Section 3 – Traitement des données à caractère personnel

Art. 6. § 1^{er}. La banque de données commune T.E.R. nécessite le traitement de différentes catégories de données à caractère personnel relatives aux personnes, aux groupements, aux organisations et aux phénomènes qui sont adéquates, pertinentes et non excessives au regard des missions visées à l'article 3, et des finalités visées à l'article 5, alinéa 2.

Les données à caractère personnel visées à l'alinéa 1^{er} présentent un lien direct avec la finalité du traitement.

§ 2. Les données à caractère personnel traitées dans la banque de données commune T.E.R. sont:

1° les données des entités suivantes:

en inzake rechten van de betrokken persoon degene bedoeld in titel 3, ondertitel 4, van dezelfde wet.

In afwijking van artikel 162 van de wet gegevensbescherming, wordt de raadpleging van persoonsgegevens en informatie geregistreerd in de gemeenschappelijke gegevensbank T.E.R. voor een verdere verwerking van de gegevens voor historische, wetenschappelijke of statistische doeleinden, toegestaan door de operationeel verantwoordelijke na overleg met de basisdiensten.

Afdeling 2 - Verwerkingsverantwoordelijken en doeleinden

Art. 5. De ministers van Binnenlandse Zaken en van Justitie zijn gezamenlijk verantwoordelijk voor de verwerking van de gemeenschappelijke gegevensbank T.E.R.

De doeleinden van de gemeenschappelijke gegevensbank T.E.R. zijn de volgende:

1° het gecoördineerde overleg tussen de basisdiensten en de partnerdiensten;

2° de strategische, tactische of operationele noodzaak om gezamenlijk persoonsgegevens en informatie te verwerken voor het uitvoeren van de respectievelijke opdrachten van de basisdiensten en de partnerdiensten;

3° de hulp bij het nemen van beslissingen door de bestuurlijke overheden of bij het nemen van beslissingen van bestuurlijke of gerechtelijke politie;

4° de analyse, de evaluatie en de opvolging, daaronder begrepen het nemen van maatregelen, van de in de gemeenschappelijke gegevensbank T.E.R. geregistreerde entiteiten en de analyse, de evaluatie en de opvolging van het fenomeen van terrorisme en extremisme wanneer het kan leiden tot terrorisme, op grond van een dreigingsevaluatie.

Afdeling 3 - Verwerking van persoonsgegevens

Art. 6. § 1. De gemeenschappelijke gegevensbank T.E.R. vereist de verwerking van verschillende categorieën van persoonsgegevens met betrekking tot personen, groeperingen, organisaties en fenomenen die toereikend, ter zake dienend en niet overmatig zijn in verhouding tot de opdrachten bedoeld in artikel 3, en de doeleinden bedoeld in artikel 5, tweede lid.

De persoonsgegevens bedoeld in het eerste lid staan in rechtstreeks verband met het doeleinde van de verwerking.

§ 2. De in de gemeenschappelijke gegevensbank T.E.R. verwerkte persoonsgegevens zijn:

1° de gegevens van de volgende entiteiten:

1) Si l'entité est une personne physique majeure ou mineure de plus de douze ans:

a) les données d'identification suivantes:

i. nom, prénoms, alias;

ii. s'il échet, le numéro d'identification du Registre national des personnes physiques;

iii. l'adresse;

iv. le genre;

v. la date, le lieu et le pays de naissance;

vi. la ou les nationalité(s);

vii. la description physique;

viii. des photos;

ix. s'il échet, la référence dactyloscopique unique;

x. l'état civil;

xi. la situation familiale;

xii. la profession;

xiii. les éléments liés à sa localisation;

xiv. les moyens de communication;

b) dans les cas déterminés par le Roi, par arrêté délibéré en Conseil de ministres, dans le but de les identifier de manière certaine, les données d'identification visées au point a), i. à xiv. des enfants mineurs biologiques ou adoptés d'une entité personne physique enregistrée dans la banque de données commune T.E.R.;

c) les données relatives aux catégories particulières de données à caractère personnel suivantes:

i. celles qui révèlent de l'origine ethnique;

ii. les opinions politiques;

iii. les convictions religieuses ou philosophiques;

iv. les données biométriques aux fins d'identifier une personne physique de manière unique;

v. les données concernant la santé;

d) les données relatives aux formations suivies;

1) Als de entiteit een meerderjarige natuurlijke persoon of een minderjarige natuurlijke persoon ouder dan twaalf jaar is:

a) de volgende indentificatiegegevens:

i. naam, voornamen, alias;

ii. indien van toepassing, het identificatienummer van het Rijksregister van de natuurlijke personen;

iii. het adres;

iv. de gender;

v. de geboortedatum, –de geboorteplaats en het geboorteland;

vi. de nationaliteit(en);

vii. de fysieke beschrijving;

viii. foto's;

ix. indien van toepassing, de unieke dactyloscopische referentie;

x. de burgerlijke staat;

xi. de gezinsituatie;

xii. het beroep;

xiii. de elementen in verband met de locatie;

xiv. de communicatiemiddelen;

b) in de gevallen bepaald door de Koning, bij een in Ministerraad overlegd besluit, om ze met zekerheid te kunnen identificeren, de onder a), i. tot en met xiv. bedoelde identificatiegegevens van de biologische of geadopteerde minderjarige kinderen van een natuurlijke persoon entiteit die in de gemeenschappelijke gegevensbank T.E.R. is geregistreerd;

c) de volgende gegevens betreffende bijzondere categorieën van persoonsgegevens:

i. de etnische afkomst;

ii. de politieke opvattingen;

iii. de godsdienstige of levensbeschouwelijke overtuiging;

iv. de biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon;

v. de gegevens over de gezondheid;

d) de gegevens met betrekking tot gevolgde opleidingen;

- e) les données relatives à la situation financière;
- f) les données relatives aux fréquentations à risque;
- g) les données relatives aux absences de réponse aux convocations de l'autorité;
- h) les moyens de transports;
- 2) si l'entité est une personne morale:
 - a) la dénomination et s'il échet l'abréviation;
 - b) le pays d'origine;
 - c) l'adresse du siège;
 - d) le type d'activités;
 - e) les éléments liés à sa localisation;
 - f) les moyens de transport;
 - g) les moyens de communication;
 - h) les personnes autorisées à l'administrer et à la représenter;
 - i) la situation juridique;

2° les données administratives, judiciaires, en ce compris celles sur les faits qualifiés d'infraction, de police judiciaire, de police administrative et les informations relatives aux entités enregistrées, traitées conformément à la loi par les services de base et les services partenaires qui disposent d'un droit de lecture et d'un droit d'écriture dans la banque de données commune T.E.R. et qui sont adéquates, pertinentes et non excessives au regard des missions visées à l'article 3 et des finalités visées à l'article 5, alinéa 2;

3° les données ou codes d'identification des personnes ou des services ayant accès à la banque de données commune T.E.R.

Les données visées à l'alinéa 1^{er}, 1°, point 1), c), v., sont traitées uniquement dans le but de comprendre le contexte médical somatique et mental lié à la personne concernée en lien direct avec les finalités visées à l'article 5, alinéa 2, ainsi que pour assurer la sécurité et protéger l'intégrité psychique et physique de toute personne susceptible d'entrer en contact avec les personnes concernées dans le cadre de l'intervention des autorités compétentes ou pour réaliser une évaluation de la menace. Lorsque des données relatives à la santé sont traitées, il est mentionné si ces données proviennent ou non de prestataires de soins.

Dans l'intérêt de la personne concernée et de celle d'un prestataire de soins, le service de base qui est en contact avec

- e) de gegevens met betrekking tot de financiële positie;
- f) de gegevens met betrekking tot risicovolle verplaatsingen;
- g) de gegevens met betrekking tot het niet reageren op de oproepingen van de autoriteit;
- h) de vervoersmiddelen;
- 2) Als de entiteit een rechtspersoon is:
 - a) de naam en, indien van toepassing, de afkorting;
 - b) het land van oorsprong;
 - c) het adres van de zetel;
 - d) de aard van de activiteiten;
 - e) de elementen met betrekking tot de locatie;
 - f) de vervoermiddelen;
 - g) de communicatiemiddelen;
 - h) de personen die bevoegd zijn om haar te beheren en te vertegenwoordigen;
 - i) de rechtstoestand;

2° de administratieve gegevens, de gerechtelijke gegevens, met inbegrip van de gegevens over strafbare feiten, de gegevens van gerechtelijke politie, de gegevens van bestuurlijke politie en de informatie betreffende de geregistreerde entiteiten, die overeenkomstig de wet verwerkt worden door de basisdiensten en de partnerdiensten die een leesrecht en een schrijfrecht hebben in de gemeenschappelijke gegevensbank T.E.R. en die toereikend, ter zake dienend en niet overmatig zijn in het licht van de opdrachten bedoeld in artikel 3 en de doeleinden bedoeld in artikel 5, tweede lid;

3° de identificatiegegevens of de identificatiecodes van de personen of de diensten die toegang hebben tot de gemeenschappelijke gegevensbank T.E.R.

De gegevens bedoeld in het eerste lid, 1°, punt 1), c), v., worden enkel verwerkt met het oog op het begrijpen van de medische somatische en geestelijke omstandigheden waarin de betrokken persoon zich bevindt, in rechtstreeks verband met de in artikel 5, lid 2, genoemde doeleinden, evenals om de veiligheid te garanderen en de psychische en fysieke integriteit te beschermen van elke persoon die in contact zou kunnen komen met de betrokken personen in het kader van de interventie door de bevoegde overheden ofwel om een dreigingsevaluatie op te stellen. Wanneer gezondheidsgegevens worden verwerkt, wordt vermeld of deze gegevens al dan niet afkomstig zijn van zorgverleners.

In het belang van de betrokken persoon en van een zorgverlener deelt de basisdienst die met laatstgenoemde in

celui-ci lui communique, les données médicales nécessaires enregistrées dans la banque de données commune T.E.R. et les données issues de l'évaluation de la menace relatives à la dangerosité de la personne concernée.

Le Roi détermine, par arrêté délibéré en Conseil des ministres, les catégories d'entités à propos desquelles les données visées à l'alinéa premier sont traitées.

Le Roi détermine, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, les mesures nécessaires en vue d'assurer la gestion et la sécurité des données à caractère personnel et des informations traitées dans la banque de données commune T.E.R.

Art. 7. § 1^{er}. Les données à caractère personnel conservées dans la banque de données commune T.E.R. sont archivées dès que les finalités visées à l'article 5, alinéa 2, ne sont plus rencontrées, et au maximum 30 ans après le dernier traitement, à l'exception des données à caractère personnel relatives à des mineurs qui sont conservées au maximum 15 ans après le dernier traitement.

Après le dernier traitement, le responsable opérationnel examine tous les cinq ans si les données à caractère personnel présentent toujours un lien direct avec l'une des finalités de l'article 5, alinéa 2. Si tel n'est pas le cas, les données sont archivées.

Lorsque les données à caractère personnel sont relatives à des mineurs, l'examen visé à l'alinéa 2 a lieu tous les trois ans.

§ 2. Les données à caractère personnel et les informations qui doivent être archivées le sont pour une durée de maximum 30 ans.

A l'issue de ce délai, ces données et informations sont supprimées, sans préjudice de la loi du 24 juin 1955 relative aux archives.

La consultation des archives de la banque de données commune T.E.R. ne peut être réalisée que dans le cadre des finalités suivantes:

1° l'appui à la définition et à la réalisation de la politique de sécurité en matière de terrorisme et d'extrémisme pouvant mener au terrorisme;

2° le traitement des antécédents dans le cadre d'une enquête judiciaire ou de renseignement de terrorisme et d'extrémisme pouvant mener au terrorisme;

3° la défense en justice des autorités visées à l'article 5, alinéa 2, 3°;

4° l'exercice des missions des autorités de contrôles, visées à l'article 30;

contact staat, hem de nodige medische gegevens mee die geregistreerd zijn in de gemeenschappelijke gegevensbank T.E.R. alsook de gegevens die afkomstig zijn van de dreigingsevaluatie met betrekking tot het gevaar dat uitgaat van de betrokken persoon.

De Koning bepaalt, bij een in Ministerraad overlegd besluit, de categorieën van entiteiten ten aanzien waarvan de in het eerste lid bedoelde gegevens verwerkt worden.

De Koning bepaalt, bij een in Ministerraad overlegd besluit en na advies van de toezichthoudende overheden, de maatregelen die nodig zijn om het beheer en de veiligheid van de persoonsgegevens en de informatie die worden verwerkt in de gemeenschappelijke gegevensbank T.E.R. te verzekeren.

Art. 7. § 1. De in de gemeenschappelijke gegevensbank T.E.R. bewaarde persoonsgegevens worden gearcheveerd vanaf het ogenblik dat de doeleinden bedoeld in artikel 5, tweede lid, niet meer worden bereikt, en ten laatste 30 jaar na de laatste verwerking, met uitzondering van de persoonsgegevens van minderjarigen, die tot maximaal 15 jaar na de laatste verwerking worden bewaard.

Na de laatste verwerking onderzoekt de operationeel verantwoordelijke om de vijf jaar of de persoonsgegevens nog steeds een rechtstreeks verband vertonen met een van de doeleinden van artikel 5, tweede lid. Indien dit niet het geval is, worden de gegevens gearcheveerd.

Wanneer de persoonsgegevens betrekking hebben op minderjarigen, vindt het in het tweede lid bedoelde onderzoek om de drie jaar plaats.

§ 2. De persoonsgegevens en de informatie die moeten worden gearcheveerd, worden gearcheveerd gedurende een termijn van maximaal 30 jaar.

Na afloop van deze termijn, worden deze gegevens en informatie gewist onverminderd de archiefwet van 24 juni 1955.

De raadpleging van de archieven van de gemeenschappelijke gegevensbank T.E.R. mag slechts gebeuren in het kader van de volgende doeleinden:

1° de ondersteuning bij het bepalen en het uitwerken van veiligheidsbeleid inzake terrorisme en extremisme dat tot terrorisme kan leiden;

2° de verwerking van de anteceden ten in het kader van een gerechtelijk onderzoek of inlichtingenonderzoek met betrekking tot een terrorisme en extremisme dat tot terrorisme kan leiden;

3° de verdediging in rechte van de overheden bedoeld in artikel 5, tweede lid, 3°;

4° de uitoefening van de opdrachten van de toezichthoudende autoriteiten als bedoeld in artikel 30;

5° la réalisation de finalités historiques, scientifiques ou statistiques.

Le résultat de l'exploitation des archives de la banque de données commune T.E.R. pour la finalité prévue à l'alinéa 3, 1°, est anonymisé.

La réalisation de finalités historiques, scientifiques ou statistiques se déroulent conformément aux dispositions du chapitre X, sous-titre 4, du Titre 3, de la loi relative à la protection des données.

§ 3. Le Roi peut, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, déterminer des règles complémentaires de gestion des données.

Art. 8. § 1^{er}. Des fichiers de journalisation sont établis dans la banque de données commune T.E.R. pour les traitements suivants: l'enregistrement de données, la modification, la consultation, la communication, y compris les transferts, l'archivage, l'interconnexion et l'effacement.

Les fichiers de journalisation de consultation et de communication permettent d'établir:

1° le motif, la date et l'heure de ces traitements;

2° les catégories de personnes qui ont consulté les données à caractère personnel, ainsi que l'identification ou le code d'identification de la personne ou du service qui a consulté ces données;

3° les systèmes qui ont communiqué ces données;

4° les catégories de destinataires des données à caractère personnel, et si possible, l'identité des destinataires de ces données.

Tous les traitements visé à l'alinéa 1^{er} dans la banque de données commune T.E.R. font l'objet d'une journalisation qui est conservée pendant 30 ans à partir du moment de leur réalisation.

Le Roi peut, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, déterminer d'autres types de traitements pour lesquels les fichiers de journalisation sont établis.

§ 2. En concertation avec le gestionnaire visé à l'article 11, le responsable opérationnel adopte des mesures appropriées pour assurer la sécurité des fichiers de journalisation et, en particulier, pour empêcher tout traitement non autorisé et pour assurer l'intégrité des données traitées.

§ 3. En concertation avec le gestionnaire visé à l'article 11, le responsable opérationnel adopte des procédures d'accès aux fichiers de journalisation, qui garantissent la nécessité et la proportionnalité de l'accès aux données de journalisation

5° de verwezenlijking van historische, wetenschappelijke of statistische doeleinden.

Het resultaat van de exploitatie van de archieven van de gemeenschappelijke gegevensbank T.E.R. voor het in het derde lid, 1°, bedoelde doeleinde wordt geanonimiseerd.

De verwezenlijking van historische, wetenschappelijke of statistische doeleinden verloopt overeenkomstig de bepalingen van hoofdstuk X, ondertitel 4, van titel 3, van de wet gegevensbescherming.

§ 3. De Koning kan, bij een in Ministerraad overlegd besluit en na advies van de toezichthoudende overheden, aanvullende regels inzake het beheer van de gegevens bepalen.

Art. 8. § 1. Logbestanden worden aangemaakt in de gemeenschappelijke gegevensbank T.E.R. voor de volgende verwerkingen: de opname van gegevens, de wijziging, de raadpleging, de mededeling, met inbegrip van de doorgiften, de archivering, de koppeling en de uitwisseling.

De logbestanden van de raadpleging en de mededeling laten toe om:

1° de beweegreden, de datum en het tijdstip van die verwerkingen vast te stellen;

2° de categorieën van personen die de persoonsgegevens hebben geraadpleegd vast te stellen, alsook de identificatie of de identificatiecode van de persoon of de dienst die deze gegevens heeft geraadpleegd;

3° vast te stellen welke systemen die gegevens hebben meegedeeld;

4° de categorieën van ontvangers van de persoonsgegevens vast te stellen en indien mogelijk de identiteit van de ontvangers van die gegevens.

Alle verwerkingen bedoeld in het eerste lid in de gemeenschappelijke gegevensbank T.E.R. zijn het voorwerp van een logging die 30 jaar wordt bijgehouden vanaf de uitvoering ervan.

De Koning kan, bij een in Ministerraad overlegd besluit en na advies van de toezichthoudende overheden, andere types van verwerking bepalen waarvoor logbestanden moeten worden opgesteld.

§ 2. In overleg met de in artikel 11 bedoelde beheerder neemt de operationeel verantwoordelijke gepaste maatregelen om de veiligheid van de logbestanden te verzekeren en, in het bijzonder om elke niet-toegelaten verwerking te beletten en de integriteit van de verwerkte gegevens te verzekeren.

§ 3. In overleg met de in artikel 11 bedoelde beheerder stelt de operationeel verantwoordelijke procedures voor toegang tot de logbestanden vast die waarborgen dat de toegang tot de logginggegevens noodzakelijk en evenredig is met het oog

en vue d'atteindre les finalités de contrôle conformément à la loi relative à la protection des données.

§ 4. Le gestionnaire visé à l'article 11 veille à la bonne exécution des dispositions visées aux paragraphes 1 à 3.

Art. 9. § 1^{er}. Dans le cadre des missions visées à l'article 3, une interconnexion peut être établie entre la banque de données commune T.E.R. et d'autres banques de données gérées par les services de base ou les services partenaires dans le cadre de leurs missions légales ou les sources authentiques de données visées au paragraphe 2.

Le Roi détermine, après avis des responsables du traitement des banques de données visées à l'alinéa 1^{er}, et pour les banques de données gérées par le partenaire visé à l'article 2, 3°, e), après accord du Collège du ministère public, les finalités de l'interconnexion, les catégories de données à caractère personnel interconnectées et les modalités d'interconnexion, lesquelles doivent respecter l'intégrité des données et des réseaux, en particulier pour ce qui concerne les banques de données qui contiennent des données classifiées au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

§ 2. Dans le cadre des missions visées à l'article 3, pour les données visées à l'article 6, § 2, alinéa 1^{er}, 1°, point 1), a), i. à xii., une interconnexion peut être établie du Registre national des personnes physiques visé à l'article 1^{er} de la loi du 8 août 1983 organisant un Registre national des personnes physique vers la banque de données commune T.E.R.

Dans le cadre des missions visées à l'article 3, pour les données visées à l'article 6, § 2, alinéa 1^{er}, 1°, point 2), a) à d), h) et i) une interconnexion peut être établie de la Banque Carrefour des Entreprises visé à l'article III.15 du Code de droit économique vers la banque de données commune T.E.R.

Dans le cadre des missions visées à l'article 3, pour les données visées à l'article 6, § 2, alinéa 1^{er}, 1°, point 1), h) et point 2), f), une interconnexion peut être établie du répertoire-matricule des véhicules visé à l'article 6 de l'arrêté royal du 20 juillet 2001 relatif à l'immatriculation de véhicules vers la banque de données commune T.E.R.

Dans le cadre des missions visées à l'article 3, pour les personnes physiques et les personnes morales enregistrées dans la banque de données commune T.E.R., une interconnexion peut être établie du Casier judiciaire central visé à l'article 589 du Code d'instruction criminelle vers la banque de données commune T.E.R.

Art. 10. Le Roi peut, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, déterminer des modalités complémentaires de gestion de la banque de données commune T.E.R.

op het bereiken van de doeleinden inzake toezicht overeenkomstig de wet gegevensbescherming.

§ 4. De in artikel 11 bedoelde beheerder ziet toe op de goede uitvoering van de bepalingen bedoeld in paragrafen 1 tot en met 3.

Art. 9. § 1. In het kader van de in artikel 3 bedoelde opdrachten kan een koppeling tot stand worden gebracht tussen de gemeenschappelijke gegevensbank T.E.R. en andere gegevensbanken die worden beheerd door de basisdiensten of de partnerdiensten in het kader van hun wettelijke opdrachten of de authentieke gegevensbronnen als bedoeld in paragraaf 2.

De Koning bepaalt, na advies van de verwerkingsverantwoordelijken van de in het eerste lid bedoeld gegevensbanken, en voor wat de gegevensbanken beheerd door de partner bedoeld in artikel 2, 3°, e), betreft, na akkoord van het College van het openbaar ministerie, de doeleinden van de koppeling, de onderling verbonden categorieën van persoonsgegevens en de nadere regels van de koppeling, waarbij de integriteit van de gegevens en van de netwerken gerespecteerd moeten worden, in het bijzonder wat betreft de gegevensbanken die geclassificeerde gegevens bevatten in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmaatregelen, veiligheidsattesten en veiligheidsadviezen.

§ 2. In het kader van de in artikel 3 bedoelde opdrachten, kan voor de gegevens bedoeld in artikel 6, § 2, eerste lid, 1°, punt 1) a), i. tot en met xii., een koppeling tot stand worden gebracht van het Rijksregister van de natuurlijke personen bedoeld in artikel 1 van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, naar de gemeenschappelijke gegevensbank T.E.R.

In het kader van de in artikel 3 bedoelde opdrachten, kan voor de gegevens bedoeld in artikel 6, § 2, eerste lid, 1°, punt 2), a) tot d), h) en i), een koppeling tot stand worden gebracht van de Kruispuntbank van Ondernemingen bedoeld in artikel III.15 van het Wetboek van economisch recht, naar de gemeenschappelijke gegevensbank T.E.R.

In het kader van de in artikel 3 bedoelde opdrachten, kan voor de gegevens bedoeld in artikel 6, § 2, eerste lid, 1°, punt 1), h) en punt 2), f), een koppeling tot stand worden gebracht van het repertorium van de voertuigen bedoeld in artikel 6 van het koninklijk besluit van 20 juli 2001 betreffende de inschrijving van voertuigen, naar de gemeenschappelijke gegevensbank T.E.R.

In het kader van de in artikel 3 bedoelde opdrachten kan, voor natuurlijke personen en rechtspersonen die in de gemeenschappelijke gegevens T.E.R. zijn geregistreerd, een koppeling tot stand worden gebracht van het Centraal Strafrechtregister bedoeld in artikel 589 van het Wetboek van Strafvordering, naar de gemeenschappelijke gegevensbank T.E.R.

Art. 10. De Koning kan, bij een in Ministerraad overlegd besluit en na advies van de toezichthoudende overheden, bijkomende nadere beheersregels van de gemeenschappelijke gegevensbank T.E.R. bepalen.

Section 4 – Gestionnaire et responsable opérationnel

Art. 11. Sur proposition conjointe des ministres de l'Intérieur et de la Justice, le Roi désigne un gestionnaire chargé de la gestion technique et fonctionnelle de la banque de données commune T.E.R.

Le gestionnaire assure au moins les missions suivantes:

1° créer et mettre à la disposition la banque de données commune T.E.R. en recourant aux moyens techniques nécessaires sur la base des possibilités découlant de l'environnement ICT propre à son service;

2° gérer la banque de données commune T.E.R. et en assurer sa maintenance;

3° traduire en règles fonctionnelles les modalités relatives au traitement de l'information;

4° déterminer les normes techniques nécessaires au fonctionnement de la banque de données commune T.E.R. et les faire appliquer;

5° fournir un avis sur le plan technique et/ou fonctionnel à la demande du responsable opérationnel ou du délégué à la protection des données visé à l'article 30;

6° organiser les droits et les accès nécessaires aux traitements à effectuer dans la banque de données commune;

7° tenir la liste des personnes ou codes d'identification des personnes ou des services ayant accès à la banque de données commune T.E.R.;

8° veiller à la journalisation des traitements réalisés dans la banque de données commune T.E.R.;

9° fournir une documentation et une assistance technique.

Art. 12. Sur proposition conjointe des ministres de l'Intérieur et de la Justice, le Roi désigne un responsable opérationnel chargé de la gestion opérationnelle de la banque de données commune T.E.R.

Le responsable opérationnel assure au moins les missions suivantes:

1° contrôler la qualité des données traitées au sein de la banque de données commune T.E.R. et s'assurer de leur pertinence au regard des finalités pour lesquelles la banque de données a été créée;

Afdeling 4 – Beheerder en operationeel verantwoordelijke

Art. 11. Op gezamenlijk voorstel van de ministers van Binnenlandse Zaken en van Justitie, wijst de Koning een beheerder aan die belast is met het technisch en functioneel beheer van de gemeenschappelijke gegevensbank T.E.R.

De beheerder verzekert minstens de volgende opdrachten:

1° het creëren en het ter beschikking stellen van de gemeenschappelijke gegevensbank T.E.R. door een beroep te doen op de noodzakelijke technische middelen op basis van de mogelijkheden die voortvloeien uit de ICT-omgeving eigen aan zijn dienst;

2° het beheren van de gemeenschappelijke gegevensbank T.E.R. en er het onderhoud van verzekeren;

3° de nadere regels met betrekking tot de verwerking van de informatie in functionele regels omzetten;

4° de technische normen bepalen die noodzakelijk zijn voor de werking van de gemeenschappelijke gegevensbank T.E.R. en deze doen toepassen;

5° een advies op technisch en/of functioneel vlak verstrekken op vraag van de operationeel verantwoordelijke of van de functionaris voor gegevensbescherming bedoeld in artikel 30;

6° de rechten en de toegangen organiseren die nodig zijn voor de te verrichte verwerkingen in de gemeenschappelijke gegevensbank T.E.R.;

7° het bijhouden van de lijst van de personen of de identificatiecodes van de personen of de diensten die over een toegang tot de gemeenschappelijke gegevensbank T.E.R. beschikken;

8° het waken over de logbestanden van de in de gemeenschappelijke gegevensbank T.E.R. uitgevoerde verwerkingen;

9° een documentatie en een technische ondersteuning aanbieden.

Art. 12. Op gezamenlijk voorstel van de ministers van Binnenlandse Zaken en van Justitie, wijst de Koning een operationeel verantwoordelijke aan die belast is met het operationeel beheer van de gemeenschappelijke gegevensbank T.E.R.

De operationeel verantwoordelijke verzekert minstens de volgende opdrachten:

1° het controleren van de kwaliteit van de in de gemeenschappelijke gegevensbank T.E.R. verwerkte gegevens en het zich verzekeren van de relevantie ervan in verhouding tot de doeleinden waarvoor de gegevensbank opgericht werd;

2° exercer une fonction de coordination pour l'alimentation de la banque de données commune T.E.R. par les différents services;

3° organiser la collaboration adéquate entre le gestionnaire, les services de base et les services partenaires en vue de réaliser les finalités prévues;

4° veiller à ce que l'exploitation des données à caractère personnel et des informations réponde aux finalités décrites à l'article 5, alinéa 2;

5° valider l'enregistrement d'une entité, dans la banque de données commune T.E.R. sur base de données et informations qui y sont introduites;

6° informer le service qui alimente la banque de données commune T.E.R. lorsque le responsable opérationnel évalue que la donnée transmise ne remplit pas ou plus un caractère adéquat, pertinent et non excessif au regard des missions visées à l'article 3, et des finalités visées à l'article 5, alinéa 2, et conclut que celle-ci doit dès lors être supprimée de la banque de données commune.

Art. 13. § 1^{er}. Le responsable opérationnel gère et traite les brèches de sécurité de la banque de données commune T.E.R. constatées personnellement ou rapportées conformément aux paragraphes 2 et 3. Pour l'application du présent article, on entend par "brèche de sécurité", toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Les brèches de sécurité de nature technique et fonctionnelle sont gérées par le gestionnaire en collaboration avec le responsable opérationnel.

§ 2. Le responsable opérationnel informe dans les plus brefs délais le gestionnaire et le délégué à la protection des données, de toute brèche de sécurité.

Le responsable opérationnel est le point de contact pour le responsable du traitement visé à l'article 5, alinéa 1^{er}, et l'informe des éventuelles brèches de sécurité.

En cas de brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable opérationnel la notifie aux autorités de contrôle dans les meilleurs délais et si possible, 72 heures après en avoir pris connaissance.

§ 3. La notification visée au paragraphe 2, alinéas 2 et 3, décrit ou communique, à tout le moins:

2° het uitoefenen van een coördinatiefunctie voor de voeding van de gemeenschappelijke gegevensbank T.E.R. door de verschillende diensten;

3° het organiseren van de passende samenwerking tussen de beheerder, de basisdiensten en de partnerdiensten met het oog op de verwezenlijking van de voorziene doeleinden;

4° erop toezien dat de exploitatie van de persoonsgegevens en de informatie beantwoordt aan de in artikel 5, tweede lid, beschreven doeleinden;

5° het valideren van de opname van een entiteit in de gemeenschappelijke gegevensbank T.E.R. op basis van gegevens en informatie die daarin worden ingevoerd;

6° het in kennis stellen van de dienst die de gemeenschappelijke gegevensbank T.E.R. voedt wanneer de operationeel verantwoordelijke oordeelt dat het doorgezonden gegeven niet of niet langer toereikend, ter zake dienend en niet-overmatig is in het licht van de opdrachten bedoeld in artikel 3 en ten opzichte van de doeleinden beoogd in artikel 5, tweede lid, en hij besluit dat dit gegeven daarom verwijderd moet worden uit de gemeenschappelijke gegevensbank.

Art. 13. § 1. De operationeel verantwoordelijke beheert en behandelt de inbreuken op de beveiliging van de gemeenschappelijke gegevensbank T.E.R. die persoonlijk worden vastgesteld of die overeenkomstig paragrafen 2 en 3 worden gerapporteerd. Voor de toepassing van dit artikel, wordt verstaan onder "inbreuk op de beveiliging", elke inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde bekendmaking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Inbreuken op de beveiliging van technische en functionele aard worden beheerd door de beheerder in samenwerking met de operationeel verantwoordelijke.

§ 2. De operationeel verantwoordelijke stelt de beheerder en de functionaris voor gegevensbescherming zo snel mogelijk in kennis van elke inbreuk op de beveiliging.

De operationeel verantwoordelijke is het contactpunt voor de verwerkingsverantwoordelijke bedoeld in artikel 5, eerste lid, en stelt hem in kennis van eventuele inbreuken op de beveiliging.

In geval van een inbreuk op de beveiliging die aanleiding kan vormen tot een hoog risico voor de rechten en vrijheden van natuurlijke personen, meldt de operationeel verantwoordelijke deze inbreuk zo snel mogelijk aan de toezichthoudende overheden en indien mogelijk, 72 uur nadat hij er kennis van heeft genomen.

§ 3. In de in paragraf 2, tweede en derde lid bedoelde melding wordt, op zijn minst, het volgende omschreven of meegedeeld:

1° la nature de la brèche de sécurité y compris, si possible, le nombre estimé de personnes et d'enregistrements de données à caractère personnel concernés;

2° le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

3° les conséquences probables de la brèche de sécurité;

4° les mesures que le responsable opérationnel a prises ou propose de prendre pour remédier à la brèche de sécurité, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Art. 14. Le Roi peut déterminer des missions spécifiques du gestionnaire et du responsable opérationnel de la banque de données commune T.E.R.

Section 5 – Droits d'accès dans la banque de données commune T.E.R.

Art. 15. Sur la base du principe du besoin d'en connaître pour l'exercice de leurs missions visées à l'article 3 et conformément aux finalités de l'article 5, alinéa 2, chacun dans le cadre de ses compétences respectives, les services de base disposent d'un droit de création, d'un droit de lecture et d'un droit d'écriture dans la banque de données commune T.E.R.

Art. 16. Dans le cadre de l'exercice de leurs missions visées à l'article 30, les autorités de contrôle disposent d'un droit de lecture dans la banque de données commune T.E.R.

Art. 17. Sur la base du principe du besoin d'en connaître pour l'exercice de leurs missions visées à l'article 3 et conformément aux finalités de l'article 5, alinéa 2, chacun dans le cadre de ses compétences respectives, les services partenaires, peuvent disposer:

1° d'un droit de lecture et d'un droit d'écriture dans la banque de données commune T.E.R.; ou

2° d'un droit d'interrogation dans la banque de données commune T.E.R.

Le Roi détermine, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, pour chaque service partenaire le type de droit et ses modalités d'exercice.

Pour le service partenaire visé à l'article 2, 3°, e), le Roi détermine, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle et avis conforme du Collège des procureurs généraux, le type de droit et ses modalités d'exercice.

1° de la nature de la brèche de sécurité y compris, si possible, le nombre estimé de personnes et d'enregistrements de données à caractère personnel concernés;

2° de la nature de la brèche de sécurité y compris, si possible, le nombre estimé de personnes et d'enregistrements de données à caractère personnel concernés;

3° de la nature de la brèche de sécurité y compris, si possible, le nombre estimé de personnes et d'enregistrements de données à caractère personnel concernés;

4° de la nature de la brèche de sécurité y compris, si possible, le nombre estimé de personnes et d'enregistrements de données à caractère personnel concernés;

Art. 14. De Koning kan bijzondere opdrachten van de beheerder en van de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank T.E.R. bepalen.

Afdeling 5 – Toegangsrechten in de gemeenschappelijke gegevensbank T.E.R.

Art. 15. Op basis van het principe van de behoefte om te kennen voor de uitoefening van hun opdrachten bedoeld in artikel 3 en overeenkomstig de doeleinden van artikel 5, tweede lid, beschikken de basisdiensten, elk in het kader van hun respectieve bevoegdheden, over een creatierecht, een leesrecht en een schrijfrecht in de gemeenschappelijke gegevensbank T.E.R.

Art. 16. In het kader van de uitoefening van hun opdrachten bedoeld in artikel 30, beschikken de toezichthoudende overheden over een leesrecht in de gemeenschappelijke gegevensbank T.E.R.

Art. 17. Op basis van het principe van de behoefte om te kennen voor de uitoefening van hun opdrachten bedoeld in artikel 3 en overeenkomstig de doeleinden van artikel 5, tweede lid, kunnen de partnerdiensten, elk in het kader van hun respectieve bevoegdheden, beschikken over:

1° een leesrecht en een schrijfrecht in de gemeenschappelijke gegevensbank T.E.R.; of

2° een vraagrecht in de gemeenschappelijke gegevensbank T.E.R.

De Koning bepaalt, bij een in Ministerraad overlegd besluit en na advies van de toezichthoudende overheden, voor iedere partnerdienst de aard van het recht en de nadere regels van de uitoefening ervan.

Voor de partnerdienst bedoeld in artikel 2, 3°, e), bepaalt de Koning, bij een in Ministerraad overlegd besluit en na advies van de toezichthoudende overheden en na eensluidend advies van het College van procureurs-generaal, de aard van het recht en de nadere regels van de uitoefening ervan.

Section 6 – Création d'une entité et alimentation de la banque de données commune T.E.R.

Art. 18. Seul un service de base dispose d'un droit de création d'une entité, dans la banque de données commune T.E.R.

Le Roi détermine, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, les modalités d'exercice du droit de création visé à l'alinéa premier.

Art. 19. Les services de base et les services partenaires, qui bénéficient d'un droit de lecture et d'un droit d'écriture sont tenus, respectivement de consulter la banque de données commune T.E.R. et d'y introduire d'office leurs propres données à caractère personnel et les informations pertinentes. Ces données à caractère personnel et informations sont enregistrées dans la banque de données commune, sous leur responsabilité et suivant leurs procédures internes de validation.

Les données à caractère personnel et informations enregistrées dans la banque de données commune T.E.R. en application de l'alinéa 1^{er} proviennent des données à caractère personnel et informations qui sont à disposition des services de base et des services partenaires dans le cadre de leurs missions respectives et des finalités qui y sont liées.

L'article 458 du Code pénal ne peut être invoqué lorsque les services de base ou les services partenaires exercent leur droit d'écriture dans la banque de données commune T.E.R. conformément à la présente section.

Les services de police saisissent les données à caractère personnel et les informations visées à l'alinéa 1^{er}, conformément aux spécifications supplémentaires énoncées dans une directive du Collège des procureurs généraux visant à sauvegarder le secret de l'instruction tel que prévu aux articles 28quinquies et 57 du Code d'instruction criminelle et l'exercice de l'action publique.

Art. 20. Par dérogation à l'article 18 et à l'article 19, alinéa 1^{er}, le droit de création et le droit d'écriture dans la banque de données commune T.E.R. sont différés lorsque et aussi longtemps que le magistrat compétent, avec l'accord du procureur fédéral, estime que cette création et cette alimentation peuvent compromettre l'exercice de l'action publique, la sécurité d'une personne ou la relation avec un service répressif d'un État étranger. Le cas échéant, le procureur fédéral peut déterminer les modalités de cette dérogation. Le procureur fédéral vérifie, à échéances régulières, la nécessité du maintien de l'ajournement de la création et de l'alimentation de la banque de données commune T.E.R.

Par dérogation à l'article 18 et à l'article 19, alinéa 1^{er}, le droit de création et le droit d'écriture dans la banque de données commune T.E.R. sont différés, lorsque et aussi longtemps que le dirigeant d'un service du renseignement et de sécurité estime que cette création et cette alimentation peuvent compromettre la sécurité d'une personne, l'exercice d'une

Afdeling 6 – Creatie van een entiteit en voeding van de gemeenschappelijke gegevensbank T.E.R.

Art. 18. Alleen een basisdienst beschikt over een creatierecht van een entiteit, in de gemeenschappelijke gegevensbank T.E.R.

De Koning bepaalt, bij een in Ministerraad overlegd besluit en na advies van de toezichhoudende overheden, de nadere regels voor het creatierecht bedoeld in het eerste lid.

Art. 19. De basisdiensten en de partnerdiensten, die een leesrecht en een schrijfrecht hebben, zijn verplicht respectievelijk de gemeenschappelijke gegevensbank T.E.R. te raadplegen en ambtshalve hun eigen persoonsgegevens en relevante informatie daarin in te voeren. Die persoonsgegevens en informatie worden onder hun verantwoordelijkheid en overeenkomstig hun interne validatieprocedures opgenomen in de gemeenschappelijke gegevensbank.

De persoonsgegevens en informatie die overeenkomstig het eerste lid in de gemeenschappelijke gegevensbank T.E.R. worden opgenomen, worden afgeleid uit de persoonsgegevens en informatie waarover de basisdiensten en de partnerdiensten beschikken in het kader van hun respectieve opdrachten en de daarmee verband houdende doeleinden.

Artikel 458 van het Strafwetboek kan niet ingeroepen worden wanneer een basisdienst of een partnerdienst in het kader van de bepalingen in deze afdeling haar schrijfrecht uitoefent in de gemeenschappelijke gegevensbank T.E.R.

De politiediensten voeren de persoonsgegevens en informatie bedoeld in het eerste lid in overeenkomstig de aanvullende specificaties vastgesteld in een richtlijn van het College van procureurs-generaal strekkende tot de vrijwaring van het geheim van het onderzoek zoals bedoeld in de artikelen 28quinquies en 57 van het Wetboek van Strafvordering en van de uitoefening van de strafvordering.

Art. 20. In afwijking van artikel 18 en artikel 19, eerste lid, worden het creatierecht en het schrijfrecht in de gemeenschappelijke gegevensbank T.E.R. uitgesteld wanneer en zolang de bevoegde magistraat, met toestemming van de federale procureur, meent dat deze creatie en deze voeding de uitoefening van de strafvordering, de veiligheid van een persoon of de relatie met een rechtshandavingsinstantie van een buitenlandse Staat in het gedrang kunnen brengen. In voorkomend geval kan de federale procureur de nadere regels voor deze afwijking bepalen. De federale procureur gaat op regelmatige tijdstippen de noodzaak tot behoud van het uitstel van de creatie en de voeding van de gemeenschappelijke gegevensbank T.E.R. na.

In afwijking van artikel 18 en artikel 19, eerste lid, worden het creatierecht en het schrijfrecht in de gemeenschappelijke gegevensbank T.E.R. uitgesteld wanneer en zolang de leidinggevende van een inlichtingen- en veiligheidsdienst meent dat deze creatie en deze voeding de veiligheid van een persoon, de uitoefening van een inlichtingenonderzoek of de relatie met

enquête de renseignement ou la relation avec un service de renseignement et de sécurité d'un État étranger.

Section 7 – Communication des données à caractère personnel et des informations

Art. 21. La fiche de renseignements est uniquement accessible aux services qui ont un droit de lecture et un droit d'écriture dans la banque de données commune T.E.R. et ne peut pas être communiquée à d'autres services ou institutions à l'exception des autorités de contrôle dans le cadre de leurs missions.

Art. 22. La création d'une nouvelle entité dans la banque de données commune T.E.R. est immédiatement communiquée au président de la Task force locale visée à l'article 31 et au chef de corps de chaque zone de police concernée. Dans le respect des conditions prévues à l'article 44/1, § 4, de la loi sur la fonction de police et en application de cet article, le chef de corps informe les autorités de police administrative compétentes.

Art. 23. Sur base du principe du besoin d'en connaître dans l'exercice de leurs missions respectives et dans le cadre des finalités visées à l'article 5, alinéa 2, les services partenaires qui, en application de l'article 17, disposent d'un droit d'interrogation dans la banque de données commune T.E.R. reçoivent l'évaluation de la menace en cas de confirmation de l'existence d'une entité dans la banque de données commune T.E.R.

Après réception de l'évaluation de la menace, le service partenaire qui a procédé à l'interrogation prend directement contact, par quelque moyen que ce soit, avec un des services de base en vue de contextualiser l'information disponible dans l'évaluation de la menace.

Art. 24. Aux fins de renforcer la prévention et la lutte contre le terrorisme et l'extrémisme pouvant mener au terrorisme, dans les limites visées à l'alinéa 2 et à l'article 25, une carte d'information peut être communiquée, à une autorité ou une institution tierce, qui a le besoin d'en connaître, après évaluation par le gestionnaire, le responsable opérationnel et les services de base, sauf décision contraire du ministère public compétent lorsque la communication des données à caractères personnel et des informations judiciaires peut compromettre l'exercice de l'action publique ou la sécurité de personnes.

L'évaluation visée à l'alinéa 1^{er} porte au minimum sur:

1° la contribution de l'autorité ou de l'institution tierce à la prévention ou à la lutte contre le terrorisme et l'extrémisme pouvant mener au terrorisme;

2° le traitement ultérieur qui sera réalisé par l'autorité ou l'institution tierce eu égard à l'exercice de ses compétences et les risques éventuels pour les libertés et droits fondamentaux de la personne concernée;

een inlichtingen- en veiligheidsdienst van een buitenlandse Staat in het gedrang kunnen brengen.

Afdeling 7 – Mededeling van de persoonsgegevens en de informatie

Art. 21. De inlichtingenfiche is enkel toegankelijk voor de diensten die een leesrecht en een schrijfrecht in de gemeenschappelijke gegevensbank T.E.R. hebben, en mag niet worden meegedeeld aan andere diensten of instellingen, met uitzondering van de toezichthoudende overheden in het kader van hun opdrachten.

Art. 22. De creatie van een nieuwe entiteit in de gemeenschappelijke gegevensbank T.E.R. wordt onverwijld meegedeeld aan de voorzitter van de Lokale Task Force bedoeld in artikel 31 en de korpschef van elke betrokken politiezone. Met naleving van de voorwaarden bepaald in en met toepassing van artikel 44/1, § 4, van de wet op het politieambt informeert de korpschef de bevoegde bestuurlijke politieoverheden.

Art. 23. Op basis van het principe van de behoefte om te kennen in het kader van de uitoefening van hun respectieve opdrachten en in het kader van de doeleinden van artikel 5, tweede lid, ontvangen de partnerdiensten die overeenkomstig artikel 17 over een vraagrecht in de gemeenschappelijke gegevensbank T.E.R. beschikken, de dreigingsevaluatie in geval van bevestiging van het bestaan van een entiteit in de gemeenschappelijke gegevensbank T.E.R.

Na ontvangst van de dreigingsevaluatie neemt de partnerdienst die tot de bevraging is overgegaan, met eender welk middel, direct contact op met een van de basisdiensten teneinde de in de dreigingsevaluatie beschikbare informatie te kunnen contextualiseren.

Art. 24. Met als doel de preventie en de bestrijding van het terrorisme en het extremisme dat tot terrorisme kan leiden, te versterken, binnen de grenzen bedoeld in het tweede lid en in artikel 25, kan, na evaluatie door de beheerder, de operationeel verantwoordelijke en de basisdiensten, een informatiekaart worden meegedeeld aan een derde overheid of instelling die de behoefte om te kennen heeft, behoudens andersluidende beslissing van het bevoegde Openbare Ministerie, wanneer de mededeling van persoonsgegevens en gerechtelijke informatie de uitoefening van de strafvordering of de veiligheid van personen in het gedrang kan brengen.

De in het eerste lid bedoelde evaluatie heeft ten minste betrekking op:

1° de bijdrage van de derde overheid of instelling tot de preventie en de bestrijding van het terrorisme en het extremisme dat tot terrorisme kan leiden;

2° de verdere verwerking die zal worden gedaan door de derde overheid of instelling rekening houdend met haar bevoegdheden en de eventuele risico's voor de fundamentele vrijheden en rechten van de betrokken persoon;

3° la situation de vulnérabilité de la personne concernée, en ce compris la minorité de la personne;

4° le caractère adéquat, pertinent et non excessif des catégories de données communiquées tenant compte du traitement ultérieur.

Art. 25. § 1^{er}. La communication visée à l'article 24 s'effectue par la transmission, par quelque moyen sécurisé que ce soit, de la carte d'information relative aux entités.

Seuls les services de base sont autorisés à transmettre la carte d'information, sans préjudice des règles et procédures applicables pour leurs propres données à caractère personnel et informations.

§ 2. Les informations émanant de la carte d'information sont utilisées par le destinataire dans le cadre de ses propres compétences légales, sans que la carte d'information ne soit ni versée au dossier de l'entité ni communiquée à celle-ci.

Art. 26. § 1^{er}. Seuls les services qui ont un droit de lecture et un droit d'écriture dans la banque de données commune T.E.R. sont autorisés à en extraire des listes de données à caractère personnel et d'informations de la carte d'information relative aux entités et ce, exclusivement pour un traitement interne. Cette extraction est effectuée par un membre du personnel titulaire d'une habilitation de sécurité "secret".

§ 2. La communication par un service de base, sous forme de listes, de données à caractère personnel ou d'informations extraites des cartes d'information, à d'autres services ou institutions, n'est pas autorisée, sauf dans les cas prévus à l'article 24. Les listes ne peuvent être communiquées qu'aux autorités publiques et services publics. La finalité de la liste s'inscrit dans les missions légales du destinataire et est précisée et communiquée au destinataire de celle-ci. L'utilisation de la liste n'est autorisée que dans le cadre de la finalité précisée. Les listes ne peuvent pas être conservées pour une durée excédant celle nécessaire à la réalisation de la finalité pour laquelle elles sont obtenues.

Art. 27. L'évaluation de la menace peut être utilisée par les services de base et les services partenaires dans le cadre de leurs propres compétences légales et conformément aux finalités de l'article 5, alinéa 2. L'évaluation de la menace peut être versée au dossier de l'entité moyennant la validation de l'Organe de coordination pour l'analyse de la menace.

L'Organe de coordination pour l'analyse de la menace actualise l'évaluation de la menace au minimum deux fois par an.

Art. 28. § 1^{er}. Les services de base sont les seuls à pouvoir communiquer les données à caractère personnel et informations de la banque de données commune T.E.R., y compris sous forme de listes, dans le cadre de communications internationales visées aux §§ 2 et 3.

3° de kwetsbare toestand van de betrokken persoon, inclusief de minderjarigheid van de persoon;

4° het toereikende, ter zake dienende en niet overmatige karakter van de categorieën van meegedeelde gegevens rekening houdend met de verdere verwerking.

Art. 25. § 1. De mededeling bedoeld in artikel 24 gebeurt door het doorzenden, met eender welk beveiligd middel van de informatiekaart met betrekking tot de entiteiten.

Onverminderd de regels en de procedures die voor hun eigen persoonsgegevens en informatie van toepassing zijn, zijn enkel de basisdiensten gemachtigd om de informatiekaart door te zenden.

§ 2. De informatie die afkomstig is van de informatiekaart, wordt door de bestemming gebruikt in het kader van zijn eigen wettelijke bevoegdheden zonder dat de informatiekaart aan het dossier van de entiteit wordt toegevoegd of aan de entiteit wordt meegedeeld.

Art. 26. § 1. Enkel de diensten met een leesrecht en een schrijfrecht in de gemeenschappelijke gegevensbank T.E.R. zijn gemachtigd om lijsten met persoonsgegevens en informatie van de informatiekaart met betrekking tot entiteiten uit de gegevensbank te halen, en zulks enkel voor interne verwerking. Deze extractie gebeurt door een personeelslid dat houder is van een veiligheidsmachtiging van het niveau "geheim".

§ 2. De mededeling aan andere diensten of instellingen door de basisdienst van persoonsgegevens of informatie gehaald uit de informatiekaarten, onder de vorm van lijsten, wordt niet toegestaan, met uitzondering van de gevallen zoals voorzien in artikel 24. De lijsten kunnen enkel meegedeeld worden aan overheidsinstanties en openbare organen. De doelstelling van de lijst kadert binnen de wettelijke opdrachten van de ontvanger en wordt bepaald en meegedeeld aan de ontvanger van de lijst. Het gebruik van de lijst wordt enkel toegestaan in het kader van deze welbepaalde doelstelling. De lijsten mogen niet langer bewaard worden dan noodzakelijk is voor de verwezenlijking van de doelstelling waarvoor zij worden verkregen.

Art. 27. De dreigingsevaluatie kan door de basisdiensten en de partnerdiensten worden gebruikt in het kader van hun eigen wettelijke bevoegdheden en overeenkomstig de doeleinden van artikel 5, tweede lid. De dreigingsevaluatie mag aan het dossier van de entiteit worden toegevoegd, onder voorbehoud van validatie door het Coördinatieorgaan voor de dreigingsanalyse.

Het Coördinatieorgaan voor de dreigingsanalyse werkt de dreigingsevaluatie ten minste tweemaal per jaar bij.

Art. 28. § 1. De basisdiensten zijn de enige diensten die de persoonsgegevens en de informatie van de gemeenschappelijke gegevensbank T.E.R. mogen meedelen, eveneens onder de vorm van lijsten, in het kader van de internationale communicatie bedoeld in §§ 2 en 3.

§ 2. Pour les missions visées à l'article 3, sans préjudice des règles internationales liant la Belgique, les données à caractère personnel et les informations de la banque de données commune T.E.R. peuvent être communiquées aux services de police étrangers et autorités judiciaires étrangères, aux organisations internationales de coopération judiciaire et policière et aux services de répression internationaux conformément à l'article 44/11/13 de la loi sur la fonction de police.

§ 3. Pour les missions visées à l'article 3, sans préjudice des règles internationales liant la Belgique, les données à caractère personnel et les informations de la banque de données commune T.E.R. peuvent être communiquées aux services de renseignement étrangers et aux organes étrangers chargés de l'analyse de la menace ou équivalents conformément à l'article 20, § 1^{er}, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et à l'article 8, 3°, de la loi du 10 juillet 2006 relative à l'analyse de la menace.

§ 4. Le Roi peut déterminer les modalités de la communication visée aux § 2 et § 3.

Section 8 – Protection des données

Art. 29. § 1^{er}. Un délégué à la protection des données est désigné conjointement par les ministres de l'Intérieur et de la Justice pour les données à caractère personnel et informations traitées dans le cadre de la banque de données commune T.E.R.

§ 2. En complément des dispositions de l'article 157 de la loi relative à la protection des données, le délégué à la protection des données est chargé:

1° de la fourniture d'avis qualifiés en matière de protection des données et de sécurisation des données à caractère personnel et informations et de leur traitement et, plus particulièrement, il veille au respect des conditions générales de licéité du traitement à l'égard des traitements de données à caractère personnel;

2° de la mise en œuvre, de la mise à jour et du contrôle d'une politique de sécurisation et de protection des données;

3° de l'exécution des autres missions relatives à la protection des données et à la sécurisation qui sont déterminées par le Roi ou qui lui sont confiées par les ministres de l'Intérieur et de la Justice.

§ 3. Le délégué à la protection des données:

1° veille à la sensibilisation des utilisateurs dans les matières de protection des données à caractère personnel et de sécurité;

2° coopère avec le gestionnaire dans le cadre de l'élaboration des procédures;

§ 2. Voor de opdrachten bedoeld in artikel 3, en onverminderd de internationale rechtsregels die België binden, kunnen de persoonsgegevens en de informatie van de gemeenschappelijke gegevensbank T.E.R. in overeenstemming met artikel 44/11/13 van de wet op het politieambt meegedeeld worden aan buitenlandse politiediensten en buitenlandse gerechtelijke autoriteiten, aan de internationale organisaties voor gerechtelijke en politionele samenwerking en aan de internationale rechtshandhavingdiensten.

§ 3. Voor de opdrachten bedoeld in artikel 3, en onverminderd de internationale rechtsregels die België binden, kunnen de persoonsgegevens en de informatie van de gemeenschappelijke gegevensbank T.E.R. in overeenstemming met artikel 20, § 1, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en artikel 8, 3°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging worden meegedeeld aan buitenlandse inlichtingendiensten en aan buitenlandse of gelijkwaardige organen belast met de dreiginganalyse.

§ 4. De Koning kan de nadere regels van de in § 2 en § 3 bedoelde mededeling bepalen.

Afdeling 8 - Gegevensbescherming

Art. 29. § 1. Een functionaris voor gegevensbescherming wordt gezamenlijk door de ministers van Binnenlandse Zaken en van Justitie aangewezen voor de persoonsgegevens en de informatie die verwerkt worden in het kader van de gemeenschappelijke gegevensbank T.E.R.

§ 2. Aanvullend op de bepalingen van artikel 157 van de wet gegevensbescherming wordt de functionaris voor gegevensbescherming belast met de volgende opdrachten:

1° het verstrekken van deskundige adviezen inzake informatieveiligheid, inzake bescherming van gegevens en informatie en inzake hun verwerking en in het bijzonder waakt hij over de eerbiediging van de algemene voorwaarden voor de rechtmatigheid van de verwerking met betrekking tot verwerkingen van persoonsgegevens;

2° het toepassen, het bijwerken en het controleren van een beleid inzake beveiliging en bescherming van gegevens;

3° het uitvoeren van andere opdrachten inzake de bescherming en beveiliging van gegevens die bepaald worden door de Koning of die hem door de ministers van Binnenlandse Zaken en Justitie worden toevertrouwd.

§ 3. De functionaris voor gegevensbescherming:

1° waakt over de bewustmaking van de gebruikers inzake bescherming van de persoonsgegevens en de veiligheid;

2° werkt samen met de beheerder in het kader van het uitwerken van procedures;

3° coopère, si nécessaire avec les délégués à la protection des données des services qui traitent des données de la banque de données commune T.E.R.;

4° est le point de contact avec les autorités de contrôle sur les questions relatives aux traitements réalisés dans la banque de données commune T.E.R.

§ 4. Le délégué à la protection des données exerce ses fonctions en toute indépendance et dans le respect des compétences et missions respectives des services de base et des services partenaires.

Le responsable du traitement visé à l'article 5, alinéa 1^{er}, le gestionnaire et le responsable opérationnel veillent à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

Le responsable du traitement visé à l'article 5, alinéa 1^{er}, veille à ce que le délégué à la protection des données dispose des ressources nécessaires pour exercer ses missions.

Le délégué à la protection des données peut être assisté par un ou plusieurs adjoints.

Il rend compte directement aux ministres de l'Intérieur et de la Justice qui en informent le responsable opérationnel.

Art. 30. § 1^{er}. La responsabilité de la qualité des données à caractère personnel, et des informations enregistrées dans la banque de données commune T.E.R. incombe:

1° au responsable du traitement propre à chaque service qui alimente la banque de données commune T.E.R. en ce qui concerne les données à caractère personnel et informations que ce service a transmises;

2° aux responsables du traitement visés à l'article 5, alinéa 1^{er}, en ce qui concerne les données à caractère personnel et informations validées sur les fiches de renseignements.

§ 2. Le responsable du traitement propre à chaque service qui alimente la banque de données commune T.E.R. veille à la légalité de la transmission de ses données à caractère personnel et informations vers la banque de données commune T.E.R.

§ 3. Le responsable du traitement visé à l'article 5, alinéa 1^{er}, veille notamment:

1° à la légalité de la transmission des données à caractère personnel et informations de la banque de données commune T.E.R.;

2° au bon fonctionnement technique et opérationnel de cette banque de données;

3° werkt, indien nodig, samen met de functionarissen voor de gegevensbescherming van de diensten die de gegevens in de gemeenschappelijke gegevensbank T.E.R. verwerken;

4° is de contactpersoon met de toezichthoudende autoriteiten voor aangelegenheden in verband met de verwerkingen die in de gemeenschappelijke gegevensbank T.E.R. worden uitgevoerd.

§ 4. De functionaris voor gegevensbescherming oefent zijn functies uit in alle onafhankelijkheid en met inachtneming van de respectieve bevoegdheden en opdrachten van de basisdiensten en de partnerdiensten.

De verwerkingsverantwoordelijke bedoeld in artikel 5, eerste lid, de beheerder en de operationeel verantwoordelijke zien erop toe dat de functionaris voor gegevensbescherming tijdig en op passende wijze betrokken wordt bij alle aangelegenheden in verband met de bescherming van persoonsgegevens.

De verwerkingsverantwoordelijke bedoeld in artikel 5, eerste lid, ziet erop toe dat de functionaris voor gegevensbescherming beschikt over de nodige middelen voor het vervullen van zijn opdrachten.

De functionaris voor gegevensbescherming kan worden bijgestaan door een of meer adjuncten.

Hij brengt rechtstreeks verslag uit aan de ministers van Binnenlandse Zaken en van Justitie, die de operationeel verantwoordelijke op de hoogte brengen.

Art. 30. § 1. De verantwoordelijkheid voor de kwaliteit van de persoonsgegevens, en de informatie die geregistreerd zijn in de gemeenschappelijke gegevensbank T.E.R., komt toe aan:

1° de verwerkingsverantwoordelijke eigen aan elke dienst die de gemeenschappelijke gegevensbank T.E.R. voedt voor wat de persoonsgegevens en informatie betreft die deze dienst heeft doorgezonden;

2° de verwerkingsverantwoordelijke bedoeld in artikel 5, eerste lid, voor wat de persoonsgegevens en informatie betreft die gevalideerd zijn op de inlichtingenfiches.

§ 2. De verwerkingsverantwoordelijke eigen aan elke dienst die de gemeenschappelijke gegevensbank T.E.R. voedt, waakt over de wettelijkheid van de doorzending van zijn persoonsgegevens en informatie naar de gemeenschappelijke gegevensbank T.E.R.

§ 3. De verwerkingsverantwoordelijke bedoeld in artikel 5 eerste lid waakt ondermeer over:

1° de wettelijkheid van de doorzending van de persoonsgegevens en informatie van de gemeenschappelijke gegevensbank T.E.R.;

2° de goede technische en operationele werking van deze gegevensbank;

3° à l'intégrité, la disponibilité et la confidentialité des données à caractère personnel et informations de la banque de données commune T.E.R. et à la sécurité des systèmes d'accès.

Il détermine par directive les mesures nécessaires en vue de satisfaire à ces obligations.

§ 4. Le Roi peut, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, déterminer d'autres règles de responsabilité en matière de protection des données à caractère personnel des services de base et des services partenaires traitant ces données.

Chapitre 3 – Enrichissement des données relatives aux entités et suivi d'une entité validée dans la banque de données commune T.E.R.

Art. 31. En vue d'assurer l'enrichissement des données à caractère personnel et informations relatives aux entités ainsi que le suivi et la prise de mesures à l'égard des entités validées dans la banque de données commune T.E.R., des données à caractère personnel et des informations enregistrées dans la banque de données commune T.E.R. ainsi que d'autres données à caractère personnel et informations pertinentes, y compris les informations classifiées au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, sont échangées au sein d'une ou plusieurs plateformes de concertation créées auprès de chaque arrondissement judiciaire, appelée Task force locale, dénommée ci-après "TFL", sauf si cet échange peut compromettre une enquête, l'exercice de l'action publique ou la sécurité de personnes.

Art. 32. § 1^{er}. La TFL est présidée par le directeur coordonnateur administratif de la police fédérale ou son représentant.

Outre le président, la TFL se compose de représentants:

- 1° des services de renseignements et de sécurité;
- 2° de l'Organe de coordination pour l'analyse de la menace;
- 3° de la police fédérale et de la police locale;
- 4° de la Direction générale de l'Office des étrangers du Service public fédéral Intérieur;
- 5° du Ministère public.

Le président et les participants à la TFL visés à l'alinéa 2, 1° à 4°, sont titulaires d'une habilitation de sécurité au moins du niveau "secret" en vertu des articles 4, 2° et 8, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

3° de integriteit, de beschikbaarheid en de vertrouwelijkheid van de persoonsgegevens en informatie van de gemeenschappelijke gegevensbank T.E.R. en de veiligheid van de toegangssystemen.

Hij bepaalt bij richtlijn de noodzakelijke maatregelen met het oog op het verzekeren van deze verplichtingen.

§ 4. De Koning kan, bij een in Ministerraad overlegd besluit en na advies van de toezichhoudende overheden, andere regels bepalen inzake de verantwoordelijkheid op het gebied van de bescherming van persoonsgegevens van de basisdiensten en de partnerdiensten die deze gegevens verwerken.

Hoofdstuk 3 – Verrijking van gegevens over entiteiten en opvolging van een in de gemeenschappelijke gegevensbank T.E.R. gevalideerde entiteit

Art. 31. Met het oog op de verrijking van persoonsgegevens en informatie over entiteiten en de opvolging en het nemen van maatregelen ten aanzien van de in de gemeenschappelijke gegevensbank T.E.R. gevalideerde entiteiten, worden er persoonsgegevens en informatie uit de gemeenschappelijke gegevensbank T.E.R., alsook andere persoonsgegevens en relevante informatie, waaronder geclassificeerde informatie in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, uitgewisseld binnen een of meer overlegplatformen die bij elk gerechtelijk arrondissement zijn opgericht, onder de naam "Lokale task force" (hierna "LTF"), tenzij die uitwisseling een onderzoek, de uitoefening van de strafvordering of de veiligheid van personen in het gedrang kan brengen.

Art. 32. § 1. De LTF wordt voorgezeten door de bestuurlijke directeur-coördinator van de federale politie of zijn vertegenwoordiger.

Naast de voorzitter, is de LTF samengesteld uit vertegenwoordigers van:

- 1° de inlichtingen- en veiligheidsdiensten;
- 2° het Coördinatieorgaan voor de dreigingsanalyse;
- 3° de federale politie en de lokale politie;
- 4° de Algemene Directie Dienst Vreemdelingenzaken van de Federale overheidsdienst Binnenlandse Zaken;
- 5° het Openbaar Ministerie.

De voorzitter en de in het tweede lid, 1° tot 4°, bedoelde deelnemers van de LTF zijn houder van een veiligheidsmachtiging ten minste van het niveau "geheim" krachtens artikelen 4, 2°, en 8, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

Le président, en concertation avec les participants à la TFL visés à l'alinéa 2, au 1° à 5°, peut inviter d'autres services, organes ou instances en raison de la contribution qu'ils peuvent apporter par leur fonction ou leurs compétences à un suivi ciblé et individualisé de l'entité.

Les services partenaires visés à l'article 2, 3°, k), seront représentés par un membre de l'administration centrale titulaire d'une habilitation de sécurité.

La coordination administrative, le secrétariat et le suivi de la TFL sont assurés par le directeur coordinateur ou les personnes qu'il désigne.

§ 2. Sans préjudice des compétences des services de base et des services partenaires, la TLF assure au moins les missions suivantes:

1° l'échange des données à caractère personnel et des informations visée à l'article 32 dans le cadre des missions visées à l'article 3;

2° le suivi des entités de la banque de données commune T.E.R. présentes sur son territoire;

3° la détermination de mesures appropriées pour chacune des entités.

Le Roi peut, par arrêté délibéré en Conseil des ministres, déterminer d'autres missions de la TFL.

Art. 33. § 1^{er}. Dès la validation d'une entité dans la banque de données commune T.E.R., sur base des données à caractère personnel et des informations visées à l'article 31, la TFL, afin d'assurer le suivi de l'entité validée, se concerta systématiquement sur l'opportunité de prendre ou non une ou plusieurs mesures visées au § 2 à l'égard de l'entité validée, sans préjudice des prérogatives des autorités compétentes pour prendre ces mesures.

Dans le cadre du suivi d'une entité, lorsque des nouvelles données à caractère personnel et informations visée à l'article 31 peuvent entraîner un changement de mesures à son égard, la TFL procède à la concertation visée à l'alinéa premier.

En vue de l'élaboration de l'approche proactive, le résultat de la concertation visée aux alinéas 1 et 2 est transmis aux autorités compétentes pour prendre les éventuelles mesures à l'égard d'une entité validée dans la banque de données commune T.E.R.

Sans préjudice de leurs prérogatives, les autorités compétentes pour prendre les mesures à l'égard d'une entité validée dans la banque de données commune prennent en considération le résultat de la concertation visée aux alinéas 1 et 2 lors de leur prise de décision.

In overleg met de in het tweede lid, 1° tot en met 5°, bedoelde deelnemers van de LTF kan de voorzitter andere diensten, organen of instanties uitnodigen wegens de bijdrage die ze door hun functie of bevoegdheden kunnen leveren aan een gerichte en geïndividualiseerde opvolging van de entiteit.

De in artikel 2, 3°, k), bedoelde partnerdiensten worden vertegenwoordigd door een lid van de centrale administratie met een veiligheidsmachtiging.

De administratieve coördinatie, het secretariaat en de opvolging van de LTF worden gewaarborgd door de directeur-coördinator of de personen die hij aanwijst.

§ 2. Onverminderd de bevoegdheden van de basisdiensten en de partnerdiensten verzekert de LTF minstens de volgende opdrachten:

1° de uitwisseling van persoonsgegevens en informatie bedoeld in artikel 32 in het kader van de opdrachten bedoeld in artikel 3;

2° de opvolging van de entiteiten van de gemeenschappelijke gegevensbank T.E.R. die op het grondgebied van de LTF aanwezig zijn;

3° de bepaling van passende maatregelen voor elk van de entiteiten.

De Koning kan, bij een in Ministerraad overlegd besluit, andere opdrachten van de LTF bepalen.

Art. 33. § 1. Vanaf de validering van een entiteit in de gemeenschappelijke gegevensbank T.E.R., op grond van de persoonsgegevens en informatie bedoeld in artikel 31, pleegt de LTF, met het oog op de opvolging van de gevalideerde entiteit, stelselmatig overleg over de opportuniteit om al dan niet een of meer maatregelen bedoeld in § 2 ten aanzien van de gevalideerde entiteit te nemen, onverminderd de prerogatieven van de bevoegde overheden om deze maatregelen te nemen.

In het kader van de opvolging van een entiteit, wanneer nieuwe persoonsgegevens en informatie bedoeld in artikel 31 tot een wijziging van maatregelen ten aanzien van de entiteit kunnen leiden, gaat de LTF over tot het overleg bedoeld in het eerste lid.

Met het oog op de uitwerking van de proactieve aanpak wordt het resultaat van het in het eerste en tweede lid bedoelde overleg bezorgd aan de overheden die bevoegd zijn om eventuele maatregelen te nemen ten aanzien van een in de gemeenschappelijke gegevensbank T.E.R. gevalideerde entiteit.

Zonder afbreuk te doen aan hun prerogatieven, nemen de overheden die bevoegd zijn om maatregelen te nemen ten aanzien van een in de gemeenschappelijke gegevensbank gevalideerde entiteit, het resultaat van het in het eerste en tweede lid bedoelde overleg in overweging bij het nemen van hun beslissing.

§ 2. La TFL se concerte notamment sur les mesures suivantes, sauf si elles peuvent compromettre une enquête, l'exercice de l'action publique ou la sécurité de personnes:

1° la mesure de signalement et de désignalement en application des dispositions en vigueur;

2° la suspension, le retrait et la restitution de cartes d'identification ou la suspension et le retrait d'autorisations qui relèvent du champ d'application de la loi du 19 juillet 1991 organisant la profession de détective privé et de la loi du 2 octobre 2017 réglementant la sécurité privée et particulière;

3° le retrait, la suspension ou la limitation d'autorisation ou d'agrément qui relèvent du champ d'application de la loi du 8 juin 2006 réglant les activités économiques et individuelles avec des armes;

4° le retrait d'habilitations, attestations et avis de sécurité qui relèvent du champ d'application de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité, attestations de sécurité et avis de sécurité;

5° la mise en place d'une enquête sociale et fiscale ou toute autre mesure spécifique dans les limites des compétences légales du Service d'information et de recherche sociale du Service public fédéral Emploi, Travail et Concertation Sociale;

6° la mise en place d'une enquête financière par la Cellule de Traitement des Informations Financières conformément à l'article 81, § 2, et l'article 83, § 2, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme;

7° la prise de mesures spécifiques dans les limites des compétences légales des services de l'Office National de l'Emploi (ONEm), l'Office wallon de la formation professionnelle et de l'emploi (FOREm), l'Office régional bruxellois de l'Emploi (Actiris), Bruxelles formation, le Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding (VDAB) et l'Arbeitsamt der Deutschsprachigen Gemeinschaft Belgiens (ADG);

8° la prise de mesures spécifiques par l'Office des étrangers en matière d'accès au territoire, de séjour, d'établissement et d'éloignement;

9° le refus, le retrait ou l'invalidation de passeport ou d'un titre de voyage belge et de documents d'identité belge conformément au Code consulaire;

10° l'inscription d'office ou la radiation d'office des registres de la population conformément à la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour;

§ 2. De LTF pleegt inzonderheid overleg over de volgende maatregelen, tenzij deze een onderzoek, de uitoefening van de strafvordering of de veiligheid van personen in het gedrang kunnen brengen:

1° de maatregel van seining en ontseining met toepassing van de inwerking zijnde bepalingen;

2° de schorsing, de intrekking en de teruggave van identificatiekaarten of de schorsing en de intrekking van vergunningen die behoren tot het toepassingsgebied van de wet van 19 juli 1991 tot regeling van het beroep van privédetective en de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid;

3° de intrekking, de schorsing of de beperking van de vergunningen of de erkenningen die behoren tot het toepassingsgebied van de wet van 8 juni 2006 houdende de regeling van economische en individuele activiteiten met wapens;

4° de intrekking van veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen die behoren tot het toepassingsgebied van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

5° de uitvoering van een sociaal en fiscaal onderzoek of enige andere specifieke maatregel binnen de grenzen van de wettelijke bevoegdheden van de Sociale Inlichtingen- en Opsporingsdienst van de Federale Overheidsdienst Werkgelegenheid, Arbeid en Sociaal Overleg;

6° de uitvoering van een financieel onderzoek door de Cel voor Financiële Informatieverwerking overeenkomstig artikel 81, § 2, en artikel 83, § 2, van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;

7° het nemen van specifieke maatregelen binnen de grenzen van de wettelijke bevoegdheden van de diensten van de Rijksdienst voor Arbeidsvoorziening (RVA), l'Office wallon de la formation professionnelle et de l'emploi (FOREm), het Brusselse Gewestelijke Dienst voor Arbeidsbemiddeling (Actiris), Bruxelles formation, de Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding (VDAB) en de Arbeitsamt der Deutschsprachigen Gemeinschaft Belgiens (ADG);

8° het nemen van specifieke maatregelen door de Dienst Vreemdelingenzaken op het gebied van toegang tot het grondgebied, verblijf, vestiging en verwijdering;

9° de weigering, de intrekking of de ongeldigverklaring van een Belgisch paspoort of reisdocument en van Belgische identiteitsdocumenten overeenkomstig het Consulair Wetboek;

10° de ambtshalve inschrijving of schrapping uit de bevolkingsregisters overeenkomstig de wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten;

11° le gel des avoirs en application de l'arrêté royal du 28 décembre 2006 relatif aux mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le financement du terrorisme;

12° le suivi effectué par les services de police dans le cadre des missions visées aux articles 14 et 15, de la loi sur la fonction de police;

13° le suivi effectué par les services de renseignements dans le cadre des missions visées aux articles 7 et 11, de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité;

14° le suivi des médias sociaux de l'entité concernée.

Chapitre 4 – Dispositions modificatives

Section 1 - Dispositions modificatives de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

Art. 34. A l'article 11, § 1^{er}, 2°, de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, les mots "à l'article 44/11/3^{ter} §§ 2 et 3, et à l'article 44/11/3^{quater} de la loi du 5 août 1992 sur la fonction de police" sont remplacés par les mots "aux articles 17 et 24, de la loi du XXX portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police".

Art. 35. Le sous-titre 4, du Titre 3, de la même loi, est complété par les mots "et dans la banque de données communes "Terrorisme, Extrémisme, processus de Radicalisation"".

Art. 36. L'article 138, § 2, de la même loi, est complété par les 8°, 9° et 10° rédigés comme suit:

8° "la loi du XXX portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.")": la loi du xxx portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police;

9° "la banque de données commune "T.E.R."": la banque de données visées à l'article 3 de la loi du XXX portant création

11° de bevroezing van de tegoeden met toepassing van het koninklijk besluit van 28 december 2006 inzake specifieke beperkende maatregelen tegen bepaalde personen en entiteiten met het oog op de strijd tegen de financiering van het terrorisme;

12° de opvolging uitgevoerd door de politiediensten in het kader van de opdrachten bedoeld in de artikelen 14 en 15 van de wet op het politieambt;

13° de opvolging uitgevoerd door de inlichtingendiensten in het kader van de opdrachten bedoeld in de artikelen 7 en 11 van de organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

14° de opvolging van de sociale media van de betrokken entiteit.

Hoofdstuk 4 – Wijzigingsbepalingen

Afdeling 1 – Wijzigingsbepalingen van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens

Art. 34. In artikel 11, § 1, 2°, van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, worden de woorden "in artikel 44/11/3^{ter}, §§ 2 en 3, en artikel 44/11/3^{quater} van de wet van 5 augustus 1992 op het politieambt" vervangen door de woorden "in de artikelen 17 en 24, van de wet van xxx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.") en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt".

Art. 35. De ondertitel 4, van titel 3, van dezelfde wet, wordt aangevuld met de woorden "en de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces"".

Art. 36. Artikel 138, § 2, van dezelfde wet, wordt aangevuld met de bepalingen onder 8°, 9° en 10°, luidende:

8° "de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.")": de wet van xxx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R."). en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt;

9° "de gemeenschappelijke gegevensbank "T.E.R."": de gegevensbank bedoeld in artikel 3 van de wet van xx tot oprichting

de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.");

10° "les responsables conjoints du traitement de la banque de données commune T.E.R.": les responsables du traitement visés à l'article 5, alinéa 1^{er}, de la loi du XXX portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.");".

Art. 37. L'article 139, alinéa 1^{er}, de la même loi, est complété par les mots "et à tout traitement de données à caractère personnel dans la banque de données commune "T.E.R."".

Art. 38. L'article 140 de la même loi est complété par un 5° rédigé comme suit:

"5° lorsque le traitement est utile dans le cadre des finalités prévues à l'article 5, alinéa 2, de la loi du XXX portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.");".

Art. 39. A l'article 143 de la même loi, les mots "l'article 44/11/3bis de la loi de 5 août 1992 sur la fonction de police en ce qui concerne les banques de données communes dont l'OCAM est le gestionnaire opérationnel." sont remplacés par les mots "l'article 7 de la loi du xx portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") en ce qui concerne la banque de données commune "T.E.R."".

Art. 40. A l'article 146, alinéa 3, de la même loi, les mots "par la loi." sont remplacés par les mots "par le Roi."

Art. 41. L'article 147 de la même loi est complété par un alinéa 2 rédigé comme suit:

"Par dérogation à l'alinéa 1^{er}, les responsables conjoints du traitement de la banque de données commune "T.E.R." tiennent un journal des demandes d'exercice des droits par les personnes concernées à l'égard des traitements effectués dans la banque de données commune "T.E.R."".

Art. 42. L'article 149, 2°, de la même loi est complété par les mots "ou dans le cadre des finalités de la banque de données commune "T.E.R." visées à l'article 5, alinéa 2, de la loi du xxx portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.");".

Art. 43. À l'article 156, § 1^{er}, de la même loi, les modifications suivantes sont apportées:

1° à l'alinéa 1^{er}, les mots "de la banque de données commune "T.E.R."", sont insérés entre les mots "de la loi du 11 décembre 1998," et les mots "des banques de données de l'OCAM";

van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.");

10° "de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R."": de verwerkingsverantwoordelijken bedoeld in artikel 5, eerste lid, van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.");".

Art. 37. Artikel 139, eerste lid, van dezelfde wet, wordt aangevuld met de woorden "en op elke verwerking van persoonsgegevens in de gemeenschappelijke gegevensbank "T.E.R."".

Art. 38. Artikel 140 van dezelfde wet, wordt aangevuld met een bepaling onder 5°, luidende:

"5° wanneer de verwerking nuttig is in het kader van de doeleinden bedoeld in artikel 5, tweede lid, van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.");".

Art. 39. In artikel 143 van dezelfde wet, worden de woorden "artikel 44/11/3bis van de wet van 5 augustus 1992 op het politieambt voor wat betreft de gemeenschappelijke gegevensbanken waarvan het OCAD de operationele beheerder is." vervangen door de woorden "artikel 7 van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.") voor wat betreft de gemeenschappelijke gegevensbank "T.E.R."".

Art. 40. In artikel 146, derde lid, van dezelfde wet, worden de woorden "in de wet" vervangen door de woorden "bij de Koning."

Art. 41. Artikel 147 van dezelfde wet word met een tweede lid aangevuld, luidende:

"In afwijking van het eerste lid, houden de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R." een logbestand bij van alle aanvragen van betrokkenen tot uitoefening van hun rechten in verband met verwerkingen die in de gemeenschappelijke gegevensbank "T.E.R." zijn verricht."

Art. 42. Artikel 149, 2°, van dezelfde wet word aangevuld met de woorden "of in het kader van de doeleinden van de gemeenschappelijke gegevensbank "T.E.R." bedoeld in artikel 5, tweede lid, van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.");".

Art. 43. In artikel 156, § 1, van dezelfde wet, worden de volgende wijzigingen aangebracht:

1° in het eerste lid, worden de woorden "van de gemeenschappelijke gegevensbank "T.E.R."", ingevoegd tussen de woorden "van de wet van 11 december 1998," en de woorden "van de gegevensbanken van het OCAD";

2° à l'alinéa 2, 1°, les mots "pour les banques de données de l'OCAM:" sont remplacés par les mots "pour la banque de données commune "T.E.R." et les banques de données de l'OCAM:".

Art. 44. L'article 158 de la même loi est remplacé comme suit:

"Art. 158. Par dérogation aux articles 20, 22, 23, 58 et 59 de la présente loi et aux articles 35 et 36 du Règlement, un protocole, un avis du délégué à la protection des données, une analyse d'impact relative à la protection des données et l'avis résultant de la consultation de l'autorité de contrôle compétente ne peuvent pas être exigés comme condition préalable à la communication de données à caractère personnel entre l'OCAM et tout organisme public ou privé dans l'intérêt de l'exercice des missions de l'OCAM.

Par dérogation aux articles 20, 22, 23, 58 et 59 de la présente loi et aux articles 35 et 36 du Règlement, un protocole, un avis du délégué à la protection des données, une analyse d'impact relative à la protection des données et l'avis résultant de la consultation de l'autorité de contrôle compétente ne peuvent pas être exigés comme condition préalable à la communication de données à caractère personnel issues de la banque de données commune "T.E.R." à tout organisme public ou privé dans l'intérêt de l'exercice des missions de prévention et de suivi du terrorisme et de l'extrémisme, lorsqu'il peut mener au terrorisme, visées à l'article 3, alinéa 1^{er}, de la loi du xx portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.").

La communication visée à l'alinéa 1^{er} se déroule conformément aux articles 8 à 12 de la loi du 10 juillet 2006.

La communication visée à l'alinéa 2 se déroule conformément aux articles 21 à 27 de la loi du xx portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.").

Par dérogation à l'article 20, paragraphe 1^{er}, alinéa 2, lorsque les parties décident de conclure un protocole, celui-ci comprend:

1° l'identification de l'OCAM et de l'organisme public ou privé qui échangent les données à caractère personnel;

2° l'identification des responsables du traitement;

3° les coordonnées des délégués à la protection des données concernés;

4° les finalités pour lesquelles les données à caractère personnel sont transférées;

5° la base légale;

2° in het tweede lid, 1°, worden de woorden "voor de gegevensbanken van het OC Opheffing" vervangen door de woorden "voor de gemeenschappelijke gegevensbank "T.E.R." en de gegevensbanken van het OCAD:".

Art. 44. Artikel 158 van dezelfde wet wordt vervangen als volgt:

"Art. 158. In afwijking van de artikelen 20, 22, 23, 58 en 59 van deze wet en van de artikelen 35 en 36 van de Verordening kan noch een protocol, noch een advies van de functionaris voor gegevensbescherming, noch een gegevensbeschermingseffectbeoordeling, noch het advies volgend op de raadpleging van de bevoegde toezichhoudende autoriteit vereist worden als voorafgaande voorwaarde voor de mededeling van persoonsgegevens tussen het OCAD en enig openbaar of particulier orgaan, in het belang van de uitvoering van de opdrachten van het OCAD.

In afwijking van de artikelen 20, 22, 23, 58 en 59 van deze wet en van de artikelen 35 en 36 van de Verordening kan noch een protocol, noch een advies van de functionaris voor gegevensbescherming, noch een gegevensbeschermingseffectbeoordeling, noch het advies volgend op de raadpleging van de bevoegde toezichhoudende autoriteit vereist worden als voorafgaande voorwaarde voor de mededeling van persoonsgegevens van de gemeenschappelijke gegevensbank "T.E.R." aan enig openbaar of particulier orgaan, in het belang van de uitvoering van de opdrachten inzake de voorkoming en de opvolging van terrorisme en extremisme, dat kan leiden tot terrorisme, bedoeld in artikel 3, eerste lid, van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.").

De mededeling bedoeld in het eerste lid vindt plaats in overeenstemming met de artikelen 8 tot 12 van de wet van 10 juli 2006.

De mededeling bedoeld in het tweede lid vindt plaats in overeenstemming met de artikelen 21 tot en met 27 van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.").

Wanneer de partijen beslissen een protocol af te sluiten, bevat dit, in afwijking van artikel 20, paragraaf 1, tweede lid, het volgende:

1° de identificatie van het OCAD en het openbaar of particulier orgaan die de persoonsgegevens uitwisselen;

2° de identificatie van de verwerkingsverantwoordelijken;

3° de contactgegevens van de betrokken functionarissen voor gegevensbescherming;

4° de doeleinden waarvoor de persoonsgegevens worden doorgegeven;

5° de wettelijke grondslag;

6° les restrictions aux droits de la personne concernée.

Le protocole visé à l'alinéa 5 porte le marquage "DIFFUSION RESTREINTE" au sens de l'arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998, pour autant qu'une classification au sens de la loi du 11 décembre 1998 ne se justifie pas."

Art. 45. L'article 161 de la même loi est complété par un alinéa 2, rédigé comme suit:

"Les autorités de contrôle visées à l'article 2, 15°, de la loi du xx portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") sont désignées conjointement comme autorités de protection des données chargées du contrôle du traitement des données à caractère personnel dans la banque de données commune "T.E.R."."

Art. 46. L'article 162 de la même loi est complété par deux alinéas rédigés comme suit:

"Par dérogation à l'alinéa 1^{er}, la consultation à des fins historiques, scientifiques ou statistiques des données à caractère personnel relatives aux entités enregistrées dans la banque de données commune T.E.R. par un responsable du traitement ultérieur est autorisée par le responsable opérationnel de la banque de données commune "T.E.R." après concertation avec les services de base visés à l'article 2, 2°, de la loi du xxx portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.").

Toute demande adressée aux Archives de l'État de traitement ultérieur de données à caractère personnel enregistrées dans la banque de données commune "T.E.R." à d'autres fins que celles visées à l'alinéa 3 est refusée à moins que la finalité soit légitime."

Art. 47. A l'article 164 de la même loi, les modifications suivantes sont apportées:

1° à l'alinéa 2, les mots "ou le responsable opérationnel de la banque de données commune "T.E.R." après concertation avec les services de base visés à l'article 2, 2°, de la loi du xxx portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") pour ce qui concerne la banque de données commune "T.E.R." sont insérés entre les mots "l'OCAM" et les mots "peut autoriser la consultation de données pseudonymisées.";

2° à l'alinéa 3, les mots "ou le responsable opérationnel de la banque de données commune "T.E.R." après concertation avec les services de base visés à l'article 2, 2°, de la loi du xxx portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") pour ce qui concerne la banque de données commune "T.E.R." sont insérés entre les mots "l'OCAM" et les mots "refuse la consultation";

6° de beperkingen van de rechten van de betrokkene.

Het protocol bedoeld in het vijfde lid draagt de markering "BEPERKTE VERSPREIDING" in de zin van het koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998, voor zover een classificatie in de zin van de wet van 11 december 1998 niet gerechtvaardigd is."

Art. 45. Artikel 161 van dezelfde wet wordt aangevuld met een tweede lid, luidende:

"De toezichthoudende overheden bedoeld in artikel 2, 15°, van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.") worden gezamenlijk aangewezen als gegevensbeschermingsautoriteiten belast met de controle van de verwerking van persoonsgegevens in de gemeenschappelijke gegevensbank "T.E.R."."

Art. 46. Artikel 162 van dezelfde wet wordt aangevuld met twee leden, luidende:

"In afwijking van het eerste lid, wordt de raadpleging voor historische, wetenschappelijke of statistische doeleinden, door een verdere verwerkingsverantwoordelijke, van persoonsgegevens met betrekking tot de in de gemeenschappelijke gegevensbank "T.E.R." geregistreerde entiteiten door de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank "T.E.R." na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.").

Elke vraag aan de Rijksarchieven om verdere verwerking van persoonsgegevens geregistreerd in de gemeenschappelijke gegevensbank "T.E.R." voor overige doelen dan die bedoeld in het derde lid wordt geweigerd tenzij het doel, legitiem is."

Art. 47. In atikel 164 van dezelfde wet, worden de volgende wijzigingen aangebracht:

1° in het tweede lid, worden de woorden "of de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank "T.E.R." na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R."), wat betreft de gemeenschappelijke gegevensbank "T.E.R.", ingevoegd tussen de woorden "het OCAD" en de woorden "de raadpleging van gepseudonimiseerde gegevens toestaan";

2° in het derde lid, worden de woorden "of de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank "T.E.R." na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R."), wat betreft de gemeenschappelijke gegevensbank "T.E.R.", ingevoegd tussen de woorden "weigert het OCAD" en de woorden "de raadpleging";

3° à l'alinéa 4, les mots "ou le responsable opérationnel de la banque de données commune "T.E.R." après concertation avec les services de base visés à l'article 2, 2°, de la loi du xxx portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") pour ce qui concerne la banque de données commune "T.E.R." sont insérés entre les mots "l'OCAM" et les mots "peut autoriser la consultation de données non pseudonymisées".

Art. 48. A l'article 165 de la même loi, les mots "ou le responsable opérationnel de la banque de données commune "T.E.R." après concertation avec les services de base visés à l'article 2, 2°, de la loi du xxx portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") pour ce qui concerne la banque de données commune "T.E.R." sont insérés entre les mots "avec l'accord de l'OCAM" et les mots "et sous les conditions que celui-ci aura fixées".

Art. 49. A l'article 166, alinéa 3, de la même loi, les 4° et 5° sont complétés par les mots "ou par le responsable opérationnel de la banque de données commune "T.E.R." après concertation avec les services de base visés à l'article 2, 2°, de la loi du xxx portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") pour ce qui concerne la banque de données commune "T.E.R.".

Section 2 - Disposition modificative de la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme

Art. 50. A l'article 4 de la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme, les modifications suivantes sont apportées:

1° dans le paragraphe 1^{er}, les mots "l'article 1^{er}, 15°, de l'arrêté royal du 23 avril 2018 relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1^{re}bis "de la gestion des informations" du chapitre IV de la loi sur la fonction de police et à l'article 1^{er}, 12°, de l'arrêté royal du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters," sont remplacés par les mots "l'article 2, 10°, de la loi du xx portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police";

2° dans le paragraphe 2, les mots "à l'article 44/11/3^{ter}, § 1^{er}, de la loi du 5 août 1992 sur la fonction de police" sont remplacés par les mots "aux articles 15 et 16, de la loi du xx portant création de la banque de données commune

3° in het vierde lid, worden de woorden "of de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank "T.E.R." na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R."), wat betreft de gemeenschappelijke gegevensbank "T.E.R.", ingevoegd tussen de woorden "kan het OCAD" en de woorden "de raadpleging van niet-gepseudonimiseerde gegevens toestaan".

Art. 48. In artikel 165 van dezelfde wet, worden de woorden "of de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank "T.E.R." na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R."), wat betreft de gemeenschappelijke gegevensbank "T.E.R.", ingevoegd tussen de woorden "met het akkoord van het OCAD" en de woorden "en onder de voorwaarden die het vastlegt".

Art. 49. In artikel 166, derde lid, van dezelfde wet, worden de bepalingen onder 4° en 5° aangevuld met de woorden "of door de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank "T.E.R." na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R."), wat betreft de gemeenschappelijke gegevensbank "T.E.R.".

Afdeling 2 – Wijzigingsbepaling van de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme

Art. 50. In artikel 4 van de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, worden de woorden "artikel 1, 15°, van het koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1^{bis} "het informatiebeheer" van hoofdstuk IV van de wet op het politieambt en artikel 1, 12°, van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Terrorist Fighters," vervangen door de woorden "artikel 2, 10°, van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.") en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt";

2° in paragraaf 2, worden de woorden "artikel 44/11/3^{ter}, § 1, van de wet van 5 augustus 1992 op het politieambt" vervangen door de woorden "artikelen 15 en 16 van de wet van xx tot oprichting van de gemeenschappelijke gegevensbank

“Terrorisme, Extrémisme, processus de Radicalisation” (“T.E.R.”) et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d’extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police”

Section 3 - Dispositions modificatives de la loi du 5 août 1992 sur la fonction de police

Art. 51. L'article 44/2, § 2, de la loi du 5 août 1992 sur la fonction de police, inséré par la loi du 27 avril 2016, est abrogé.

Art. 52. Dans le chapitre IV, section 12, de la même loi, la sous-section 7*bis*, comportant les articles 44/11/3*bis* à 44/11/3*quinqüies*/2, insérée par la loi du 27 avril 2016 et modifiée par la loi du 22 mai 2019, est abrogée.

Art. 53. Dans le chapitre IV, section 12, sous-section 8, de la même loi, insérée par la loi du 18 mars 2014 et modifiée en dernier lieu par la loi du 31 juillet 2020, il est inséré un article 44/11/9*bis*, rédigé comme suit:

“Art. 44/11/9*bis*. Lorsque dans leurs missions de police administrative ou de police judiciaire, les membres des services de police sont appelés à coopérer avec les services de la santé, d'urgence et/ou de secours, ils peuvent communiquer des données à caractère personnel et des informations pour autant qu'elles soient adéquates, pertinentes et strictement nécessaires pour permettre aux membres des services de la de santé, d'urgence et/ou de secours, d'effectuer leurs missions dans des conditions de sécurité optimales et d'assurer la sécurité et l'intégrité psychologique et physique de toute personne dans l'exercice de ces fonctions.”

Chapitre 5 – Dispositions finales

Art. 54. Le Roi peut remplacer les références existantes dans les lois aux dispositions de la loi sur la fonction de police par les références aux dispositions correspondantes de la présente loi.

Le Roi peut remplacer les références existantes dans les lois aux dispositions de l'arrêté royal du 21 juillet 2016 relatif à la banque de données commune “Terrorist Fighters” et de l'arrêté royal du 23 avril 2018 relatif à la banque de données commune “Propagandistes de haine” et portant exécution de certaines dispositions de la section 1*re bis* “de la gestion des informations” du chapitre IV de la loi sur la fonction de police, par les références aux dispositions correspondantes des arrêtés d'exécution de la présente loi.

Art. 55. Pour les entités enregistrées dans la banque de données communes visée à l'article 44/2, § 2, de la loi sur la fonction de police au moment de l'entrée en vigueur de la présente loi, la TFL procède à la concertation visée à l'article 33, § 1^{er}, lorsque de nouvelles données à caractère

“Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”) en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt”.

Afdeling 3 – Wijzigingsbepalingen van de wet van 5 augustus 1992 op het politieambt

Art. 51. Artikel 44/2, § 2, van de wet van 5 augustus 1992 op het politieambt, ingevoegd bij de wet van 27 april 2016, wordt opgeheven.

Art. 52. In hoofdstuk IV, afdeling 12, van dezelfde wet, wordt de onderafdeling 7*bis*, dat de artikelen 44/11/3*bis* tot 44/11/3*quinqüies*/2 bevat, ingevoegd bij de wet van 27 april 2016 en gewijzigd bij de wet van 22 mei 2019, opgeheven.

Art. 53. In hoofdstuk IV, afdeling 12, onderafdeling 8, van dezelfde wet van 5 augustus 1992 op het politieambt, ingevoegd bij de wet van 18 maart 2014 en laatste gewijzigd bij de wet van 31 juli 2020 wordt een artikel 44/11/9*bis* ingevoegd, luidende:

“Art. 44/11/9*bis*. Wanneer de leden van de politiediensten in het kader van hun opdrachten van bestuurlijke of gerechtelijke politie moeten samenwerken met de gezondheids-, hulp- en/of reddingsdiensten, kunnen zij persoonsgegevens en informatie meedelen voor zover deze toereikend, ter zake dienend en strikt noodzakelijk zijn om de leden van de gezondheids-, hulp- en/of reddingsdiensten in staat te stellen hun taken in optimale veiligheidsomstandigheden uit te voeren en om de veiligheid en de psychische en fysieke integriteit te waarborgen van eenieder bij de uitvoering van die taken.”

Chapitre 5 - Slotbepalingen

Art. 54. De Koning kan de bestaande verwijzingen in wetten naar bepalingen van de wet op het politieambt vervangen door verwijzingen naar de ermee overeenstemmende bepalingen van deze wet.

De Koning kan de bestaande verwijzingen in wetten naar bepalingen van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Terrorist Fighters en het koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1*bis* “Het informatiebeheer” van hoofdstuk IV van de wet op het politieambt, vervangen door verwijzingen naar de ermee overeenstemmende bepalingen van de koninklijke besluiten van deze wet.

Art. 55. De LTF gaat, voor de entiteiten die op het ogenblik van de inwerkingtreding van deze wet in de gemeenschappelijke gegevensbanken zoals bedoeld in artikel 44/2, § 2, van de wet op het politieambt zijn opgenomen, over tot het bij artikel 33, § 1, ingevoerd overleg wanneer nieuwe persoonsgegevens

personnel et informations visée à l'article 31 peuvent entraîner un changement de mesures à l'égard de l'entité concernée.

Art. 56. La présente loi entre en vigueur à la date fixée par le Roi et au plus tard le xx/xx/xxxx

en informatie zoals bedoeld in artikel 31 kunnen leiden tot een verandering van maatregelen ten aanzien van de betrokken entiteit.

Art. 56. Deze wet treedt in werking op de datum bepaald door de Koning en uiterlijk op xxx

AVIS DU CONSEIL D'ÉTAT N° 73.442/2 DU 7 JUIN 2023

Le 12 avril 2023, le Conseil d'État, section de législation, a été invité par le Vice-Premier ministre et ministre de la Justice et de la Mer du Nord à communiquer un avis, dans un délai de trente jours, sur un avant-projet de loi 'portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police'.

L'avant-projet a été examiné par la deuxième chambre le 7 juin 2023. La chambre était composée de Pierre VANDERNOOT, président de chambre, Patrick RONVAUX et Christine HOREVOETS, conseillers d'État, Sébastien VAN DROOGHENBROECK, assesseur, et Esther CONTI, greffier assumé.

Le rapport a été présenté par Véronique SCHMITZ, premier auditeur.

La concordance entre la version française et la version néerlandaise de l'avis a été vérifiée sous le contrôle de Pierre VANDERNOOT.

L'avis, dont le texte suit, a été donné le 7 juin 2023.

*

Comme la demande d'avis est introduite sur la base de l'article 84, § 1^{er}, alinéa 1^{er}, 2^o, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, la section de législation limite son examen au fondement juridique de l'avant-projet[†], à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, l'avant-projet appelle les observations suivantes.

FORMALITÉS PRÉALABLES

Même si, depuis la modification des lois coordonnées 'sur le Conseil d'État' par la loi du 2 avril 2003 'modifiant certains aspects de la législation relative à l'organisation et au fonctionnement de la section de législation du Conseil d'État', le non-accomplissement des formalités ne peut plus conduire à l'irrecevabilité des demandes d'avis, il n'en reste pas moins qu'en principe la section de législation ne peut être consultée qu'à l'issue des différentes étapes de la préparation administrative de l'avant-projet concerné et après que l'organe compétent pour l'établissement de celui-ci a

[†] S'agissant d'amendements à un projet de loi, on entend par "fondement juridique" la conformité aux normes supérieures.

ADVIES VAN DE RAAD VAN STATE NR. 73.442/2 VAN 7 JUNI 2023

Op 12 april 2023 is de Raad van State, afdeling Wetgeving, door de Vice-eersteminister en minister van Justitie en Noordzee verzocht binnen een termijn van dertig dagen een advies te verstrekken over een voorontwerp van wet 'tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.") en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidszellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt'.

Het voorontwerp is door de tweede kamer onderzocht op 7 juni 2023. De kamer was samengesteld uit Pierre VANDERNOOT, kamervoorzitter, Patrick RONVAUX en Christine HOREVOETS, staatsraden, Sébastien VAN DROOGHENBROECK, assessor, en Esther CONTI, toegevoegd griffier.

Het verslag is uitgebracht door Véronique SCHMITZ, eerste auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Pierre VANDERNOOT.

Het advies, waarvan de tekst hierna volgt, is gegeven op 7 juni 2023.

*

Aangezien de adviesaanvraag is ingediend op basis van artikel 84, § 1, eerste lid, 2^o, van de wetten 'op de Raad van State', gecoördineerd op 12 januari 1973, beperkt de afdeling Wetgeving overeenkomstig artikel 84, § 3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond van het voorontwerp,[‡] de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

Wat die drie punten betreft, geeft het voorontwerp aanleiding tot de volgende opmerkingen.

VOORAFGAANDE VORMVEREISTEN

Sinds de wijziging van de gecoördineerde wetten 'op de Raad van State' bij de wet van 2 april 2003 'tot wijziging van sommige aspecten van de wetgeving met betrekking tot de inrichting en de werkwijze van de afdeling wetgeving van de Raad van State', kan de niet-vervulling van vormvereisten er weliswaar niet meer toe leiden dat adviesaanvragen onontvankelijk zijn maar het beginsel blijft dat de afdeling Wetgeving pas om advies kan worden gevraagd nadat het betrokken voorontwerp alle achtereenvolgende stadia van de administratieve voorbereiding heeft doorlopen en nadat het orgaan dat

[‡] Aangezien het om amendementen op een wetsontwerp gaat, wordt onder "rechtsgrond" de overeenstemming met de hogere rechtsnormen verstaan.

eu la possibilité de l'adapter éventuellement à la lumière des éléments recueillis lors de l'accomplissement des formalités. Il serait ainsi évité que le Conseil d'État donne son avis sur un projet de texte non définitif et il serait garanti que l'avis soit rendu sur la base d'une information complète concernant tous les éléments pertinents en cause¹.

Cette observation s'applique *a fortiori* pour l'avis de l'Organe de Contrôle de l'Information Policière (ci-après: "le C.O.C.") lorsqu'il s'agit d'avant-projets qui, comme celui à l'examen, concernent par excellence le traitement de données à caractère personnel, l'obligation consultative ayant précisément pour objectif de vérifier notamment si le régime en projet est bien conforme aux exigences juridiques imposées en matière de traitement de données à caractère personnel². Il en va de même pour l'avis de l'Autorité de protection des données (ci-après: "l'A.P.D."), également requis. Dans la lettre de demande d'avis, il est par ailleurs mentionné que d'autres avis ont été sollicités mais ceux-ci n'ont pas été transmis à la section de législation du Conseil d'État: il s'agit des avis du Collège des Procureurs généraux, de l'Ordre des médecins et des délégués généraux aux droits de l'enfant.

Il ressort des mesures d'instruction prises par l'auditeur-rapporteur que ces avis n'ont pas encore été donnés.

La méthode consistant à saisir simultanément la section de législation du Conseil d'État, le C.O.C. et l'A.P.D. est donc, en l'espèce, particulièrement critiquable³. Elle ne permet en effet pas à la section de législation de disposer de l'ensemble des informations pertinentes pouvant être utiles à son examen, plus précisément sur la manière dont il aurait été tenu compte de ces avis et dont cette prise en compte aurait été traduite dans l'exposé des motifs et dans le commentaire des articles.

¹ Avis 41.417/AG à 41.420/AG donné le 6 octobre 2006 sur des avant-projets devenus respectivement la loi du 10 mai 2007 'modifiant la loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme et la xénophobie', la loi du 10 mai 2007 'tendant à lutter contre la discrimination entre les femmes et les hommes', la loi du 10 mai 2007 'tendant à lutter contre certaines formes de discrimination' et la loi du 10 mai 2007 'adaptant le Code judiciaire à la législation tendant à lutter contre les discriminations et réprimant certains actes inspirés par le racisme ou la xénophobie' (*Doc. parl.*, Chambre, 2006-2007, n° 51-2720/001, p. 126).

² En ce sens également, l'avis 69.369/1 donné le 4 juin 2021 sur un avant-projet devenu l'ordonnance de la Commission communautaire commune du 27 janvier 2022 'modifiant l'ordonnance du 11 mai 2017 concernant le parcours d'accueil des primo-arrivants' (*Doc. parl.*, Parl. Rég. Brux.-Cap., 2021-2022, n° B-87/1, pp. 9 et s.).

³ Voir en ce sens notamment l'avis 71.258/2 donné le 4 mai 2022 sur un avant-projet devenu la loi du 16 octobre 2022 'visant la création du Registre central pour les décisions de l'ordre judiciaire et relative à la publication des jugements et modifiant la procédure d'assises relative à la récusation des jurés', observation préalable n° 2 (*Doc. parl.*, Chambre, 2021-2022, n° 55-2754/001, pp. 68 et s.). Voir également l'avis 72.873/2 donné le 15 mai 2023 sur un avant-projet de loi 'modifiant la loi sur la fonction de police' (non publié à la date à laquelle le présent avis est donné).

bevoegd is om het voorontwerp vast te stellen de mogelijkheid heeft gehad het eventueel aan te passen in het licht van de elementen die bij het vervullen van de vormvereisten naar voren zijn gekomen. Aldus wordt vermeden dat de Raad van State advies zou uitbrengen over een niet-definitieve ontwerp tekst en wordt gewaarborgd dat het advies kan worden uitgebracht met volledige kennis van alle ter zake relevante elementen.¹

Die opmerking geldt *a fortiori* voor het advies van het Controleorgaan op de politieke informatie (afgekort en hierna: "het COC") wanneer het om ontwerpen gaat die, zoals het voorliggende voorontwerp, bij uitstek betrekking hebben op de verwerking van persoonsgegevens: de adviesverplichting strekt er precies toe onder meer na te gaan of de ontworpen regeling wel in overeenstemming is met de juridische vereisten die gelden voor de verwerking van persoonsgegevens². Hetzelfde geldt voor het – eveneens vereiste – advies van de Gegevensbeschermingsautoriteit (hierna: "de GBA"). In de brief met de adviesaanvraag wordt bovendien vermeld dat nog om andere adviezen is verzocht maar dat die niet zijn overgezonden aan de afdeling Wetgeving van de Raad van State: het gaat om de adviezen van het College van procureurs-generaal, de Orde der artsen en de algemeen afgevaardigden voor de rechten van het kind.

Uit het onderzoek van de auditeur-rapporteur blijkt dat die adviezen nog niet gegeven zijn.

De methode die erin bestaat tegelijk het advies van de afdeling Wetgeving van de Raad van State, van het COC en van de GBA aan te vragen, is *in casu* dan ook ten zeerste af te keuren.³ De afdeling Wetgeving kan dan immers niet over alle relevante informatie beschikken die mogelijk nuttig is voor haar onderzoek, meer in het bijzonder betreffende de wijze waarop met die adviezen rekening zou zijn gehouden en hoe dit in de memorie van toelichting en in de artikelsgewijze bespreking naar voren zou zijn gebracht.

¹ Adviezen 41.417/AV tot 41.420/AV van 6 oktober 2006 over voorontwerpen die hebben geleid tot respectievelijk de wet van 10 mei 2007 'tot wijziging van de wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden', de wet van 10 mei 2007 'ter bestrijding van discriminatie tussen vrouwen en mannen', de wet van 10 mei 2007 'ter bestrijding van bepaalde vormen van discriminatie' en de wet van 10 mei 2007 'tot aanpassing van het Gerechtelijk Wetboek aan de wetgeving ter bestrijding van discriminatie en tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden' (*Parl. St. Kamer* 2006-07, nr. 51-2720/001, 126).

² Zie in die zin eveneens advies 69.369/1 van 4 juni 2021 over een voorontwerp dat heeft geleid tot de ordonnantie van de Gemeenschappelijke Gemeenschapscommissie van 27 januari 2022 'tot wijziging van de ordonnantie van 11 mei 2017 betreffende het inburgeringstraject voor de nieuwkomers' (*Parl. St. Br. Parl.* 2021-22, nr. B-87/1, 9 e.v.).

³ Zie in die zin onder meer advies 71.258/2 van 4 mei 2022 over een voorontwerp dat heeft geleid tot de wet van 16 oktober 2022 'tot oprichting van het Centraal register voor de beslissingen van de rechterlijke orde en betreffende de bekendmaking van de vonnissen en tot wijziging van de assisenprocedure betreffende de wraking van de gezworenen', voorafgaande opmerking 2 (*Parl. St. Kamer* 2021-22, nr. 55-2754/001, 68 e.v.). Zie eveneens advies 72.873/2 van 15 mei 2023 over een voorontwerp van wet 'tot wijziging van de wet op het politieambt' (niet bekendgemaakt op de datum waarop dit advies wordt gegeven).

En tout état de cause, l'exposé des motifs doit fournir des éclaircissements quant à la manière dont les avis du C.O.C. et de l'A.P.D. auront été pris en compte par l'avant-projet.

Enfin, si l'examen par l'auteur de l'avant-projet de ces avis devait encore donner lieu à des modifications du texte soumis au Conseil d'État sur des points autres que de pure forme ou ne résultant pas également des suites réservées au présent avis, les dispositions modifiées ou ajoutées devraient être soumises à nouveau à l'avis de la section de législation conformément à l'article 3, § 1^{er}, alinéa 1^{er}, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973.

Observations préalables sur la portée de l'examen de l'avant-projet

1. La lettre de demande d'avis est rédigée de la manière suivante:

"Le projet de loi que je sou mets à votre avis vise tout d'abord à transposer dans une loi autonome les dispositions relatives aux banques de données communes qui sont actuellement décrites à la sous-section 7bis 'Des banques de données communes' de la loi du 5 août 1992 sur la fonction de police et dans les arrêtés royaux du 21 juillet 2016 relatif à la banque de données communes 'Terrorist Fighters' et du 23 avril 2018 relatif à la banque de données commune 'Propagandistes de haine'.

Ce projet de loi est d'un part constitué de dispositions transférées sans modification de fond de la loi sur la fonction de police, ainsi que des [arrêtés royaux] 'Terrorist Fighters' et 'Propagandistes de haine'.

D'autre part, ce projet apporte des définitions et des précisions sur la notion d'entité enregistrée dans la banque de données commune (BDC) T.E.R., précise les différents types de supports d'extraits de données contenues dans la BDC T.E.R., précise les règles liées aux traitements de données des mineurs, énumère les catégories de données à caractère personnel qui peuvent être traitées dans la BDC TER, permet la communication de données enregistrées dans la BDC TER aux professionnels des soins de santé, prévoit que l'analyse de la menace d'une entité devra être mise à jour au moins deux fois par an, permet l'interconnexion de la banque de données commune avec d'autres banques de données et précise le fonctionnement des local task forces.

Ensuite, la loi cadre en matière de protection des données (loi du 30 juillet 2018) a été modifiée pour donner un traitement juridique clair aux données à caractère personnel concaténées par différents services au sein d'une même banque de données.

Enfin, la loi sur la fonction de police a également été adaptée afin de donner une assise juridique claire à la coopération et la communication de données entre les différents services (services de police, services d'urgence et de secours et services de la santé) qui doivent intervenir en réponse à des incidents mineurs ou majeurs et, en particulier, à garantir

In de memorie van toelichting moet hoe dan ook worden verduidelijkt hoe in het voorontwerp rekening zou zijn gehouden met de adviezen van het COC en de GBA.

Indien de aan de Raad van State voorgelegde tekst, ingevolge het onderzoek van die adviezen door de steller van het voorontwerp, nog wijzigingen zou ondergaan die niet louter vormelijk zijn of die niet eveneens voortvloeien uit het gevolg dat aan dit advies wordt gegeven, moeten de gewijzigde of toegevoegde bepalingen ten slotte opnieuw om advies aan de afdeling Wetgeving worden voorgelegd overeenkomstig artikel 3, § 1, eerste lid, van de wetten 'op de Raad van State', gecoördineerd op 12 januari 1973.

VOORAFGAANDE OPMERKINGEN OVER DE DRAAGWIJDTE VAN HET ONDERZOEK VAN HET VOORONTWERP

1. De brief met de adviesaanvraag is gesteld als volgt:

"Le projet de loi que je sou mets à votre avis vise tout d'abord à transposer dans une loi autonome les dispositions relatives aux banques de données communes qui sont actuellement décrites à la sous-section 7bis 'Des banques de données communes' de la loi du 5 août 1992 sur la fonction de police et dans les arrêtés royaux du 21 juillet 2016 relatif à la banque de données communes 'Terrorist Fighters' et du 23 avril 2018 relatif à la banque de données commune 'Propagandistes de haine'.

Ce projet de loi est d'un part constitué de dispositions transférées sans modification de fond de la loi sur la fonction de police, ainsi que des [arrêtés royaux] 'Terrorist Fighters' et 'Propagandistes de haine'.

D'autre part, ce projet apporte des définitions et des précisions sur la notion d'entité enregistrée dans la banque de données commune (BDC) T.E.R., précise les différents types de supports d'extraits de données contenues dans la BDC T.E.R., précise les règles liées aux traitements de données des mineurs, énumère les catégories de données à caractère personnel qui peuvent être traitées dans la BDC TER, permet la communication de données enregistrées dans la BDC TER aux professionnels des soins de santé, prévoit que l'analyse de la menace d'une entité devra être mise à jour au moins deux fois par an, permet l'interconnexion de la banque de données commune avec d'autres banques de données et précise le fonctionnement des local task forces.

Ensuite, la loi cadre en matière de protection des données (loi du 30 juillet 2018) a été modifiée pour donner un traitement juridique clair aux données à caractère personnel concaténées par différents services au sein d'une même banque de données.

Enfin, la loi sur la fonction de police a également été adaptée afin de donner une assise juridique claire à la coopération et la communication de données entre les différents services (services de police, services d'urgence et de secours et services de la santé) qui doivent intervenir en réponse à des incidents mineurs ou majeurs et, en particulier, à garantir

l'intégrité physique et psychologique de la personne concernée elle-même et de toute personne susceptible d'entrer en contact avec elle dans le cadre de l'intervention des services précités et la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme, a été légèrement adaptée purement pour des questions de forme et de renvoi.

Le projet d'arrêté royal quant à lui rassemble dans un seul instrument plusieurs arrêtés royaux qui étaient relatifs à la banque de données commune et les rassemble dans un seul instrument".

L'exposé des motifs explique que sont rassemblées au niveau législatif dans un texte autonome les dispositions légales et réglementaires existantes pour donner une base juridique *ad hoc* à la banque de données commune T.E.R., qui est commune à différents services et qui n'avait donc pas de raison spécifique d'être attachée à la loi du 5 août 1992 'sur la fonction de police', mais aussi parce que, "dans un souci d'une plus grande sécurité juridique, bon nombre de dispositions jugées essentielles qui se trouvaient énoncées dans les arrêtés royaux créant les banques de données 'Terrorist Fighters' et 'Propagandistes de haine' ont été ramenées au niveau de la loi".

Techniquement, il ressort du commentaire de l'article 2 que la banque de données commune T.E.R. correspond à l'actuelle banque de données commune "Terrorist fighters" et "Propagandistes de haine"⁴ car, "dans les faits, au niveau informatique [...], il existe une seule et même banque de données commune pour toutes les catégories de personnes et entités listées dans les arrêtés royaux du 21 juillet 2016 et du 23 avril 2018 précités"⁵.

2. Il en résulte que, pour les dispositions qui sont reproduites des textes existants sans modification de fond^{6,7} tout en précisant la nouvelle appellation de la banque de données commune "T.E.R.", il est renvoyé aux avis qui ont été donnés par la section de législation sur ces dispositions.

Pour les dispositions relatives à la loi du 5 août 1992 'sur la fonction de police' et à ses arrêtés d'exécution, il s'agit principalement des avis 58.729/AG donné le 26 janvier 2016 sur un avant-projet devenu la loi du 27 avril 2016 'relative à des mesures complémentaires en matière de lutte contre

l'intégrité physique et psychologique de la personne concernée elle-même et de toute personne susceptible d'entrer en contact avec elle dans le cadre de l'intervention des services précités et la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme, a été légèrement adaptée purement pour des questions de forme et de renvoi.

Le projet d'arrêté royal quant à lui rassemble dans un seul instrument plusieurs arrêtés royaux qui étaient relatifs à la banque de données commune et les rassemble dans un seul instrument."

In de memorie van toelichting wordt uitgelegd dat de bestaande wettelijke en verordenende bepalingen worden samengebracht in een op zichzelf staande wetgevende tekst teneinde een ad-hocrechtsgrondslag te geven aan de gemeenschappelijke gegevensbank T.E.R., die gemeenschappelijk is voor verschillende diensten en dus niet specifiek aan de wet van 5 augustus 1992 'op het politieambt' gekoppeld diende te zijn, maar ook omdat, "ter wille van een grotere rechtszekerheid, heel wat essentieel geachte bepalingen die in de koninklijke besluiten tot oprichting van de gegevensbanken 'Terrorist Fighters' en 'Haatpropagandisten' waren opgenomen, [worden] vastgelegd in de wet".

Uit de bespreking van artikel 2 blijkt dat, technisch gesproken, de gemeenschappelijke gegevensbank T.E.R. bestaat uit de huidige gemeenschappelijke gegevensbanken "Terrorist Fighters" en "Haatpropagandisten"⁴ want "in feite [bestaat er] vanuit informatica oogpunt (...) slechts één gemeenschappelijke gegevensbank voor alle categorieën van personen of entiteiten die in de voornoemde koninklijke besluiten van 21 juli 2016 en 23 april 2018 worden opgesomd".⁵

2. Dientengevolge wordt, wat de bepalingen betreft die zonder wezenlijke wijziging^{6,7} worden overgenomen uit de bestaande teksten maar die wel de precisering bevatten betreffende de nieuwe benaming van de gemeenschappelijke gegevensbank "T.E.R.", verwezen naar de adviezen die de afdeling Wetgeving over die bepalingen heeft gegeven.

Voor de bepalingen betreffende de wet van 5 augustus 1992 'op het politieambt' en betreffende de besluiten tot uitvoering van die wet, gaat het hoofdzakelijk om de adviezen 58.729/AV van 26 januari 2016 over een voorontwerp dat heeft geleid tot de wet van 27 april 2016 'inzake aanvullende maatregelen ter

⁴ Voir, dans le commentaire de l'article 2, le point 6), "Banque de données commune T.E.R."

⁵ Exposé des motifs et commentaire de l'article 3.

⁶ L'exposé des motifs comporte des explications à cet égard.

⁷ Les articles 51 et 52 de l'avant-projet ont pour objet, par voie de conséquence, d'abroger respectivement l'article 44/2, § 2, de la loi du 5 août 1992 'sur la fonction de police', inséré par la loi du 27 avril 2016 'relative à des mesures complémentaires en matière de lutte contre le terrorisme', et, dans le chapitre IV, section 12, de la loi du 5 août 1992, la sous-section 7bis, comportant les articles 44/11/3bis à 44/11/3quinquies/2, insérée par la loi du 27 avril 2016 et modifiée par la loi du 22 mai 2019 'modifiant diverses dispositions en ce qui concerne la gestion de l'information policière'.

⁴ Zie punt 6), "Gemeenschappelijke gegevensbank T.E.R." in de bespreking van artikel 2.

⁵ Memorie van toelichting en bespreking van artikel 3.

⁶ De memorie van toelichting geeft daar uitleg over.

⁷ De artikelen 51 en 52 van het voorontwerp strekken dientengevolge tot opheffing van respectievelijk artikel 44/2, § 2, van de wet van 5 augustus 1992 'op het politieambt', ingevoegd bij de wet van 27 april 2016 'inzake aanvullende maatregelen ter bestrijding van terrorisme', en, in hoofdstuk IV, afdeling 12, van de wet van 5 augustus 1992, van onderafdeling 7bis, met daarin de artikelen 44/11/3bis tot 44/11/3quinquies/2, ingevoegd bij de wet van 27 april 2016 en gewijzigd bij de wet van 22 mei 2019 'tot wijziging van diverse bepalingen wat het politionele informatiebeheer betreft'.

le terrorisme⁸, 59.515/2 donné le 6 juillet 2016 sur un projet devenu l'arrêté royal du 21 juillet 2016 'relatif à la banque de données commune *Terrorist Fighters* et portant exécution de certaines dispositions de la section 1^{re}bis "de la gestion des informations" du chapitre IV de la loi sur la fonction de police', 62.629/2 et 62.630/2 donnés le 31 janvier 2018 sur deux projets devenus respectivement l'arrêté royal du 23 avril 2018 'modifiant l'arrêté royal du 21 juillet 2016 relatif à la banque de données commune *Foreign Terrorist Fighters* portant exécution de certaines dispositions de la section 1^{re}bis "de la gestion des informations" du chapitre IV de la loi sur la fonction de police et modifiant la banque de données commune *Foreign Terrorist Fighters* vers la banque de données commune *Terrorist Fighters*' et l'arrêté royal du 23 avril 2018 'relatif à la banque de données commune *Propagandistes de haine* et portant exécution de certaines dispositions de la section 1^{re}bis "de la gestion des informations" du chapitre IV de la loi sur la fonction de police'. Pour les dispositions de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel' qui sont complétées ou auxquelles il est renvoyé, il s'agit de l'avis 63.192/2 donné le 19 avril 2018 sur un avant-projet devenu cette loi précitée^{9,10}. Il en va de même pour l'avis 63.480/2 donné le 6 juin 2018 sur un avant-projet devenu la loi du 30 juillet 2018 'portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme'^{11,12}.

Le tableau de correspondance des articles, l'exposé des motifs et le commentaire des articles seront complétés par la référence aux avis précités.

3. Un projet d'arrêté royal 'relatif à la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.")' a été soumis à l'avis de la section de législation concomitamment à l'avant-projet de loi à l'examen.

L'avis 73.443/2 du 3 mai 2023 a déclaré cette demande d'avis prématurée au motif que le projet d'arrêté royal se

bestrijding van terrorisme⁸, 59.515/2 van 6 juli 2016 over een ontwerp dat heeft geleid tot het koninklijk besluit van 21 juli 2016 'betreffende de gemeenschappelijke gegevensbank *Terrorist Fighters* en tot uitvoering van sommige bepalingen van de afdeling 1bis "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt', 62.629/2 en 62.630/2 van 31 januari 2018 over twee ontwerpen die hebben geleid tot respectievelijk het koninklijk besluit van 23 april 2018 'betreffende de gemeenschappelijke gegevensbank *Foreign Terrorist Fighters* en tot uitvoering van sommige bepalingen van de afdeling 1bis "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt en tot omvorming van de gemeenschappelijke gegevensbank *Foreign Terrorist Fighters* naar de gemeenschappelijke gegevensbank *Terrorist Fighters*' en het koninklijk besluit van 23 april 2018 'betreffende de gemeenschappelijke gegevensbank *Haatpropagandisten* en tot uitvoering van sommige bepalingen van de afdeling 1bis "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt' en 66.662/2 van 25 november 2019 over een ontwerp dat heeft geleid tot het koninklijk besluit van 20 december 2019 'tot wijziging van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank *Terrorist Fighters* en van het koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank *Haatpropagandisten* en tot uitvoering van sommige bepalingen van de afdeling 1bis "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt'. Wat betreft de bepalingen van de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens' die worden aangevuld of waarnaar wordt verwezen, gaat het om advies 63.192/2 van 19 april 2018 over een voorontwerp dat heeft geleid tot die voornoemde wet.^{9,10} Hetzelfde geldt voor advies 63.480/2 van 6 juni 2018 over een voorontwerp dat heeft geleid tot de wet van 30 juli 2018 'tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme'^{11,12}.

De tabel met de overeenstemming tussen de artikelen, de memorie van toelichting en de bespreking van de artikelen moeten worden aangevuld met een verwijzing naar de voornoemde adviezen.

3. Gelijktijdig met het voorliggende voorontwerp van wet is een ontwerp van koninklijk besluit 'betreffende de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.")' aan de afdeling Wetgeving voorgelegd.

In advies 73.443/2 van 3 mei 2023 werd gesteld dat die adviesaanvraag voorbarig was omdat als rechtsgrond voor dat

⁸ *Doc. parl.*, Chambre, 2015-2016, n° 54-1727/001, pp. 89 et s.

⁹ *Doc. parl.*, Chambre, 2017-2018, n° 54-3126/001, pp. 402 et s.

¹⁰ Les articles 34 à 49 complètent, pour la banque de données commune T.E.R., les dispositions existantes de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel'.

¹¹ *Doc. parl.*, Chambre, 2017-2018, n° 54-3209/001, pp. 14 et s.

¹² L'article 50 a pour seul objet d'adapter les renvois contenus dans l'article 4 de la loi du 30 juillet 2018 'portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme'.

⁸ *Parl.St.* Kamer 2015-16, nr. 54-1727/001, 89 e.v.

⁹ *Parl.St.* Kamer 2017-18, nr. 54-3126/001, 402 e.v.

¹⁰ De artikelen 34 tot 49 strekken tot aanvulling, wat de gemeenschappelijke gegevensbank T.E.R. betreft, van de bestaande bepalingen van de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens'.

¹¹ *Parl.St.* Kamer 2017-18, nr. 54-3209/001, 14 e.v.

¹² Artikel 50 strekt alleen tot aanpassing van de verwijzingen vervat in artikel 4 van de wet van 30 juli 2018 'tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme'.

donnait pour fondement légal des dispositions législatives figurant dans l'avant-projet faisant l'objet du présent avis, par hypothèse non encore adoptées¹³.

En raison de la conception d'un nouveau texte législatif autonome rassemblant des dispositions légales et réglementaires existantes, il convient de prévoir que les dispositions qui sont issues des arrêtés royaux du 21 juillet 2016 'relatif à la banque de données communes "Terrorist Fighters"'¹⁴ et du 23 avril 2018 'relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1^{re} bis "de la gestion des informations" du chapitre IV de la loi sur la fonction de police' seront abrogées à la même date que la date d'entrée en vigueur de l'avant-projet.

OBSERVATIONS GÉNÉRALES

I. — Quant au cadre général relatif à l'admissibilité de restrictions aux droits et libertés fondées sur la lutte contre le terrorisme

La banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") implique des restrictions au droit au respect à la vie privée garanti par l'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme.

Dans son avis 58.729/AG donné le 26 janvier 2016 sur un avant-projet devenu la loi du 27 avril 2016 'relative à des mesures complémentaires en matière de lutte contre le terrorisme', la section de législation a rappelé ce qui suit:

"La lutte contre le terrorisme fait incontestablement partie des motifs légitimes pouvant justifier des restrictions à ces libertés.

Ainsi, appelée à examiner les restrictions apportées aux droits de l'homme sur cette base, la Cour européenne des droits de l'homme

'rappelle qu'elle est pleinement consciente des difficultés que les États rencontrent pour protéger leur population contre la violence terroriste, laquelle constitue en elle-même

ontwerp van koninklijk besluit wetgevende bepalingen werden opgegeven die in het voorontwerp staan waarover dit advies gegeven wordt, en die *a fortiori* nog niet waren aangenomen.¹³

Aangezien een nieuwe op zichzelf staande wetgevende tekst wordt ontworpen die bestaande wettelijke en verordenende bepalingen samenbrengt, dient te worden voorzien dat de bepalingen die afkomstig zijn van het koninklijk besluit van 21 juli 2016 'betreffende de gemeenschappelijke gegevensbank Terrorist Fighters'¹⁴ en van het koninklijk besluit van 23 april 2018 'betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1bis "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt' worden opgeheven op dezelfde datum als de datum van inwerkingtreding van het voorontwerp.

ALGEMENE OPMERKINGEN

I. — Algemeen kader waarbinnen beperkingen van rechten en vrijheden op grond van de bestrijding van terrorisme kunnen worden aanvaard

De gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.") impliceert beperkingen van het recht op eerbiediging van het privéleven, dat wordt gewaarborgd bij artikel 22 van de Grondwet en artikel 8 van het Europees Verdrag voor de rechten van de mens.

In advies 58.729/AV van 26 januari 2016 over een voorontwerp dat heeft geleid tot de wet van 27 april 2016 'inzake aanvullende maatregelen ter bestrijding van terrorisme' heeft de afdeling Wetgeving op het volgende gewezen:

"De bestrijding van terrorisme is onmiskenbaar één van de wettige redenen die beperkingen van die vrijheden kunnen rechtvaardigen.

Toen het Europees Hof voor de Rechten van de Mens zich diende te buigen over de beperkingen die op grond daarvan aan de rechten van de mens werden opgelegd, heeft dat Hof eraan herinnerd

'qu'elle est pleinement consciente des difficultés que les États rencontrent pour protéger leur population contre la violence terroriste, laquelle constitue en elle-même une grave menace

¹³ Cet avis n'est pas encore publié à la date à laquelle le présent avis est donné.

¹⁴ En vertu de l'article 1^{er} de l'arrêté royal du 23 avril 2018 'modifiant l'arrêté royal du 21 juillet 2016 relatif à la banque de données commune *Foreign Terrorist Fighters* portant exécution de certaines dispositions de la section 1^{re} bis "de la gestion des informations" du chapitre IV de la loi sur la fonction de police et modifiant la banque de données commune *Foreign Terrorist Fighters* vers la banque de données commune *Terrorist Fighters*', "[l']intitulé de l'arrêté royal du 21 juillet 2016 relatif à la banque de données commune *Foreign Terrorist Fighters* et portant exécution de certaines dispositions de la section 1^{re} bis "de la gestion des informations" du chapitre IV de la loi sur la fonction de police est remplacé par ce qui suit: 'Arrêté royal relatif à la banque de données commune *Terrorist Fighters*'".

¹³ Dat advies is op de datum waarop dit advies wordt gegeven, nog niet bekendgemaakt.

¹⁴ Krachtens artikel 1 van het koninklijk besluit van 23 april 2018 'tot wijziging van het Koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank *Foreign Terrorist Fighters* en tot uitvoering van sommige bepalingen van de afdeling 1bis "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt en tot omvorming van de gemeenschappelijke gegevensbank *Foreign Terrorist Fighters* naar de gemeenschappelijke gegevensbank *Terrorist Fighters*', "[wordt] het opschrift van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank *Foreign Terrorist Fighters* en tot uitvoering van sommige bepalingen van de afdeling 1bis "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt (...) vervangen als volgt: 'Koninklijk besluit betreffende de gemeenschappelijke gegevensbank *Terrorist Fighters*'".

une grave menace pour les droits de l'homme. Elle se garde donc de sous-estimer l'ampleur du danger que représente le terrorisme et la menace qu'il fait peser sur la collectivité (*Othman (Abu Qatada) c. Royaume-Uni*, n° 8139/09, § 183, CEDH 2012 (extraits), et références citées). Elle considère qu'il est légitime, devant une telle menace, que les États contractants fassent preuve d'une grande fermeté à l'égard de ceux qui contribuent à des actes de terrorisme (*idem*)¹⁵.

Il est également renvoyé à l'arrêt *Szabo et Vissy c. Hongrie* prononcé le 12 janvier 2016 par la Cour européenne des droits de l'homme, qui propose une synthèse récente relative aux normes et principes de protection de la vie privée en matière de lutte contre le terrorisme.

Les lignes directrices du Comité des ministres du Conseil de l'Europe 'sur les droits de l'homme et la lutte contre le terrorisme', établissent de la manière suivante l'équilibre à établir entre les intérêts de la collectivité et les droits individuels en cause¹⁶:

'Le Comité des ministres,

[a.] Considérant que le terrorisme porte gravement atteinte aux droits de l'homme, menace la démocratie et vise notamment à déstabiliser des gouvernements légitimement constitués et à saper la société civile pluraliste;

[b.] Condamnant catégoriquement comme criminels et injustifiables tous les actes, méthodes ou pratiques terroristes, où qu'ils se produisent et quels qu'en soient les auteurs;

[c.] Rappelant qu'un acte terroriste ne peut jamais être excusé ou justifié en invoquant les droits de l'homme et que l'abus de droit n'est jamais protégé;

[d.] Rappelant qu'il est non seulement possible, mais absolument nécessaire, de lutter contre le terrorisme dans le respect des droits de l'homme, de la prééminence du droit et, lorsqu'il est applicable, du droit international humanitaire;

[e.] Rappelant la nécessité pour les États de tout mettre en œuvre, et notamment de coopérer, afin que les auteurs, organisateurs et commanditaires présumés d'actes terroristes soient traduits en justice pour répondre de toutes les conséquences, notamment pénales et civiles, de leurs actes;

[f.] Réaffirmant le devoir impératif des États de protéger les populations contre d'éventuels actes terroristes;

[g.] Rappelant la nécessité pour les États, notamment pour des raisons d'équité et de solidarité sociale, de veiller

pour les droits de l'homme. Elle se garde donc de sous-estimer l'ampleur du danger que représente le terrorisme et la menace qu'il fait peser sur la collectivité (*Othman (Abu Qatada) c. Royaume-Uni*, n° 8139/09, § 183, CEDH 2012 (extraits), et références citées). Elle considère qu'il est légitime, devant une telle menace, que les États contractants fassent preuve d'une grande fermeté à l'égard de ceux qui contribuent à des actes de terrorisme (*idem*)¹⁵.

Er wordt eveneens verwezen naar het arrest *Szabo en Vissy t. Hongarije* dat op 12 januari 2016 door het Europees Hof voor de Rechten van de Mens is uitgesproken en waarin een actuele synthese wordt gemaakt van de rechtsregels en de beginselen met betrekking tot de bescherming van de persoonlijke levenssfeer die van toepassing zijn op het vlak van de bestrijding van terrorisme.

In de richtsnoeren van het Comité van ministers van de Raad van Europa 'over de rechten van de mens en de bestrijding van terrorisme' wordt over het evenwicht dat moet worden nagestreefd tussen de belangen van de samenleving in haar geheel en de in het geding zijnde individuele rechten het volgende vermeld:¹⁶

'Le Comité des ministres,

[a.] Considérant que le terrorisme porte gravement atteinte aux droits de l'homme, menace la démocratie et vise notamment à déstabiliser des gouvernements légitimement constitués et à saper la société civile pluraliste;

[b.] Condamnant catégoriquement comme criminels et injustifiables tous les actes, méthodes ou pratiques terroristes, où qu'ils se produisent et quels qu'en soient les auteurs;

[c.] Rappelant qu'un acte terroriste ne peut jamais être excusé ou justifié en invoquant les droits de l'homme et que l'abus de droit n'est jamais protégé;

[d.] Rappelant qu'il est non seulement possible, mais absolument nécessaire, de lutter contre le terrorisme dans le respect des droits de l'homme, de la prééminence du droit et, lorsqu'il est applicable, du droit international humanitaire;

[e.] Rappelant la nécessité pour les États de tout mettre en œuvre, et notamment de coopérer, afin que les auteurs, organisateurs et commanditaires présumés d'actes terroristes soient traduits en justice pour répondre de toutes les conséquences, notamment pénales et civiles, de leurs actes;

[f.] Réaffirmant le devoir impératif des États de protéger les populations contre d'éventuels actes terroristes;

[g.] Rappelant la nécessité pour les États, notamment pour des raisons d'équité et de solidarité sociale, de veiller

¹⁵ Note de bas de page n° 10 de l'avis cité: Cour eur. D. H., not. arrêt *Trabelsi c. Belgique*, 4 septembre 2014, § 117.

¹⁶ Note de bas de page n° 11 de l'avis cité: Seules les parties les plus pertinentes en l'espèce de ces lignes directrices sont reproduites ci-après.

¹⁵ Voetnoot 10 van het geciteerde advies: EHRM inzonderheid 4 september 2014, *Trabelsi t. België*, § 117.

¹⁶ Voetnoot 11 van het geciteerde advies: Hierna worden alleen de *in casu* meest relevante passages van die richtsnoeren opgenomen.

à ce que les victimes d'actes terroristes puissent obtenir un dédommagement;

[h.] Gardant à l'esprit que la lutte contre le terrorisme implique des mesures à long terme visant à prévenir les causes du terrorisme, en favorisant notamment la cohésion de nos sociétés et le dialogue multiculturel et inter-religieux;

[i.] Réaffirmant l'obligation des États de respecter, dans leur lutte contre le terrorisme, les instruments internationaux de protection des droits de l'homme, et pour les États membres, tout particulièrement la Convention de Sauvegarde des Droits de l'Homme et des Libertés fondamentales ainsi que la jurisprudence de la Cour européenne des Droits de l'Homme;

Adopte les lignes directrices suivantes et invite les États membres à en assurer une large diffusion auprès de toutes les autorités chargées de la lutte contre le terrorisme.

I. *Obligation des États de protéger toute personne contre le terrorisme* - Les États ont l'obligation de prendre les mesures nécessaires pour protéger les droits fondamentaux des personnes relevant de leur juridiction à l'encontre des actes terroristes, tout particulièrement leur droit à la vie. Cette obligation positive justifie pleinement la lutte des États contre le terrorisme, dans le respect des présentes lignes directrices.

II. *Interdiction de l'arbitraire* - Les mesures prises par les États pour lutter contre le terrorisme doivent respecter les droits de l'homme et le principe de la prééminence du droit, en excluant tout arbitraire ainsi que tout traitement discriminatoire ou raciste, et faire l'objet d'un contrôle approprié.

III. *Légalité des mesures anti-terroristes* - 1. Toute mesure prise par les États pour lutter contre le terrorisme doit avoir une base juridique.

2. Lorsqu'une mesure restreint les droits de l'homme, les restrictions doivent être définies de façon aussi précise que possible et être nécessaires et proportionnées au but poursuivi.

[...]

V. *Collecte et traitement de données à caractère personnel par toute autorité compétente en matière de sécurité de l'État* - Dans le cadre de la lutte contre le terrorisme, la collecte et le traitement de données à caractère personnel par toute autorité compétente en matière de sécurité de l'État ne peuvent porter atteinte au respect de la vie privée des personnes que si la collecte et le traitement sont, notamment:

(i) régis par des dispositions appropriées en droit interne;

(ii) proportionnés à l'objectif pour lequel cette collecte et ce traitement ont été prévus;

(iii) susceptibles d'un contrôle par une autorité externe indépendante.

VI. *Mesures d'ingérence dans la vie privée* - 1. Les mesures dans la lutte contre le terrorisme qui constituent une ingérence

à ce que les victimes d'actes terroristes puissent obtenir un dédommagement;

[h.] Gardant à l'esprit que la lutte contre le terrorisme implique des mesures à long terme visant à prévenir les causes du terrorisme, en favorisant notamment la cohésion de nos sociétés et le dialogue multiculturel et inter-religieux;

[i.] Réaffirmant l'obligation des États de respecter, dans leur lutte contre le terrorisme, les instruments internationaux de protection des droits de l'homme, et pour les États membres, tout particulièrement la Convention de Sauvegarde des Droits de l'Homme et des Libertés fondamentales ainsi que la jurisprudence de la Cour européenne des Droits de l'Homme;

Adopte les lignes directrices suivantes et invite les États membres à en assurer une large diffusion auprès de toutes les autorités chargées de la lutte contre le terrorisme.

I. *Obligation des États de protéger toute personne contre le terrorisme* - Les États ont l'obligation de prendre les mesures nécessaires pour protéger les droits fondamentaux des personnes relevant de leur juridiction à l'encontre des actes terroristes, tout particulièrement leur droit à la vie. Cette obligation positive justifie pleinement la lutte des États contre le terrorisme, dans le respect des présentes lignes directrices.

II. *Interdiction de l'arbitraire* - Les mesures prises par les États pour lutter contre le terrorisme doivent respecter les droits de l'homme et le principe de la prééminence du droit, en excluant tout arbitraire ainsi que tout traitement discriminatoire ou raciste, et faire l'objet d'un contrôle approprié.

III. *Légalité des mesures anti-terroristes* - 1. Toute mesure prise par les États pour lutter contre le terrorisme doit avoir une base juridique.

2. Lorsqu'une mesure restreint les droits de l'homme, les restrictions doivent être définies de façon aussi précise que possible et être nécessaires et proportionnées au but poursuivi.

(...)

V. *Collecte et traitement de données à caractère personnel par toute autorité compétente en matière de sécurité de l'État* - Dans le cadre de la lutte contre le terrorisme, la collecte et le traitement de données à caractère personnel par toute autorité compétente en matière de sécurité de l'État ne peuvent porter atteinte au respect de la vie privée des personnes que si la collecte et le traitement sont, notamment:

(i) régis par des dispositions appropriées en droit interne;

(ii) proportionnés à l'objectif pour lequel cette collecte et ce traitement ont été prévus;

(iii) susceptibles d'un contrôle par une autorité externe indépendante.

VI. *Mesures d'ingérence dans la vie privée* - 1. Les mesures dans la lutte contre le terrorisme qui constituent une ingérence

dans la vie privée (notamment, les fouilles, les perquisitions, les écoutes, les écoutes téléphoniques, la surveillance de la correspondance et le recours à l'infiltration d'agents) doivent être prévues par la loi. Ces mesures doivent pouvoir faire l'objet d'un contrôle juridictionnel.

2. Les mesures prises pour lutter contre le terrorisme doivent être préparées et contrôlées par les autorités de façon à réduire au minimum, autant que faire se peut, le recours à la force meurtrière et, dans ce cadre, l'utilisation d'armes par les forces de sécurité doit être rigoureusement proportionnée à la défense d'autrui contre la violence illégale ou à la nécessité de procéder à une arrestation régulière.

VII. *Arrestation et garde à vue* - 1. L'arrestation d'une personne soupçonnée d'activités terroristes ne peut intervenir en l'absence de soupçons plausibles. Les motifs de l'arrestation doivent être communiqués à la personne arrêtée.

2. Une personne arrêtée ou détenue pour activités terroristes doit être aussitôt traduite devant un juge. La garde à vue doit être d'une durée raisonnable et son terme doit être fixé par la loi.

3. Une personne arrêtée ou détenue pour activités terroristes doit pouvoir contester la légalité de son arrestation ou de sa garde à vue devant un tribunal.

[...]¹⁷.

C'est à la lumière de ces règles et principes, tels qu'ils ont encore été rappelés par l'arrêt *Big Brother Watch et autres c. Royaume-Uni* prononcé le 25 mai 2021 par la Cour européenne des droits de l'homme en Grande Chambre, que doivent également être examinées les dispositions de l'avant-projet en ce qu'elles complètent un dispositif juridique existant en matière de lutte contre le terrorisme.

Plus particulièrement, il s'agit par exemple des nouvelles dispositions qui ont pour objet d'ajouter des services partenaires à la liste existante figurant dans la loi du 5 août 1992 'sur la fonction de police' (article 2, 3°, de l'avant-projet), du fait que les catégories d'entités sont déterminées par le Roi (articles 2, 4°, et 6, § 2, alinéa 4, de l'avant-projet), qu'une "entité" peut être un mineur de plus de douze ans (lire: "douze ans et plus")¹⁸ (article 2, 4°, de l'avant-projet) ou que la banque de données commune T.E.R. peut contenir des données relatives à un mineur (article 6, § 2, alinéa 1^{er}, 1°, 1), b), de l'avant-projet), de l'ajout de la finalité de la concertation coordonnée entre les services de base et les services partenaires (article 5, alinéa 2, 1°, de l'avant-projet), de la récolte des données santé et de la communication au prestataire de soins (article 6, § 2, alinéas 2 et 3, de l'avant-projet), des délais de conservation différents pour les données relatives aux mineurs (article 7, § 1^{er}, de l'avant-projet), de l'interconnexion à d'autres banques de données dont des sources authentiques (article 7 de

dans la vie privée (notamment, les fouilles, les perquisitions, les écoutes, les écoutes téléphoniques, la surveillance de la correspondance et le recours à l'infiltration d'agents) doivent être prévues par la loi. Ces mesures doivent pouvoir faire l'objet d'un contrôle juridictionnel.

2. Les mesures prises pour lutter contre le terrorisme doivent être préparées et contrôlées par les autorités de façon à réduire au minimum, autant que faire se peut, le recours à la force meurtrière et, dans ce cadre, l'utilisation d'armes par les forces de sécurité doit être rigoureusement proportionnée à la défense d'autrui contre la violence illégale ou à la nécessité de procéder à une arrestation régulière.

VII. *Arrestation et garde à vue* - 1. L'arrestation d'une personne soupçonnée d'activités terroristes ne peut intervenir en l'absence de soupçons plausibles. Les motifs de l'arrestation doivent être communiqués à la personne arrêtée.

2. Une personne arrêtée ou détenue pour activités terroristes doit être aussitôt traduite devant un juge. La garde à vue doit être d'une durée raisonnable et son terme doit être fixé par la loi.

3. Une personne arrêtée ou détenue pour activités terroristes doit pouvoir contester la légalité de son arrestation ou de sa garde à vue devant un tribunal.

(...)¹⁷.

In zoverre de bepalingen van het voorontwerp een bestaand juridisch dispositief inzake terrorismebestrijding aanvullen, moeten ze eveneens worden onderzocht in het licht van die regels en beginselen, zoals die nog in herinnering zijn gebracht in arrest-*Big Brother Watch e.a. t. Verenigd Koninkrijk*, uitgesproken op 25 mei 2021 door de Grote Kamer van het Europees Hof voor de Rechten van de Mens.

Meer in het bijzonder gaat het bijvoorbeeld om de nieuwe bepalingen die ertoe strekken partnerdiensten toe te voegen aan de bestaande lijst die is opgenomen in de wet van 5 augustus 1992 'op het politieambt' (artikel 2, 3°, van het voorontwerp), om het feit dat de categorieën van entiteiten worden bepaald door de Koning (artikelen 2, 4°, en 6, § 2, vierde lid, van het voorontwerp), dat een "entiteit" een minderjarige ouder dan twaalf jaar kan zijn (lees: "van twaalf jaar en ouder")¹⁸ (artikel 2, 4°, van het voorontwerp) of dat de gemeenschappelijke gegevensbank T.E.R. gegevens kan bevatten over een minderjarige (artikel 6, § 2, eerste lid, 1°, 1), b), van het voorontwerp). Voorts gaat het om de toevoeging van de doelstelling van het gecoördineerde overleg tussen de basisdiensten en de partnerdiensten (artikel 5, tweede lid, 1°, van het voorontwerp), het verzamelen van gezondheidsgegevens en de mededeling aan de zorgverlener (artikel 6, § 2, tweede en derde lid, van het voorontwerp), de verschillende termijnen voor de bewaring van de gegevens over minderjarigen

¹⁷ Avis 58.729/AG donnée le 26 janvier 2016 sur un avant-projet devenu la loi du 27 avril 2016 'relative à des mesures complémentaires en matière de lutte contre le terrorisme' (*Doc. parl.*, Chambre, 2015-2016, n° 54-1727/001, pp. 89 et s.).

¹⁸ Observation particulière n° 2 formulée sous l'article 2.

¹⁷ Advies 58.729/AV van 26 januari 2016 over een voorontwerp dat heeft geleid tot de wet van 27 april 2016 'inzake aanvullende maatregelen ter bestrijding van terrorisme' (*Parl. St.* Kamer 2015-16, nr. 54-1727/001, 89 e.v.).

¹⁸ Bijzondere opmerking 2 bij artikel 2.

l'avant-projet), de la notion de "brèches de sécurité" (article 13 de l'avant-projet), de la circonstance que l'évaluation de la menace est communiquée aux services partenaires lors de l'exercice du droit d'interrogation (article 23 de l'avant-projet), de la description du contenu de l'évaluation qui doit être effectuée avant la communication de la carte d'information à une autorité ou à une institution tierce (article 24, alinéa 2, de l'avant-projet), de la validation de l'évaluation de la menace par l'OCAM (article 27, alinéa 1^{er}, de l'avant-projet) ou encore de la création des "Task force locales", en abrégé "TFL", qui rassemblent des professionnels de la sécurité afin d'examiner l'opportunité de la prise de mesures à l'égard d'une "entité" enregistrée (articles 31 à 33 de l'avant-projet).

II. — Quant au traitement de données à caractère personnel

A. L'articulation des règles en matière de protection des données contenues dans l'avant-projet avec celles figurant dans la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel'

L'avant-projet, d'une part, élabore un dispositif autonome à la loi 'sur la fonction de police'¹⁹, dont l'objet est de porter création de la banque de données commune T.E.R. et, d'autre part, modifie notamment des dispositions dans la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel'.

Le commentaire des articles 4 et 34 précise ce qui suit à ce sujet:

"Le présent avant-projet de loi règle les questions en matière de protection des données qui sont propres aux traitements de données au sein de la banque de données commune T.E.R., à savoir quels types de données à caractère personnel y sont traitées, pour quelles finalités, pendant combien de temps, qui est responsable du traitement, quelles autorités doivent alimenter la banque de données, avec quelles catégories de données, quelles sont les catégories d'autorités qui peuvent recevoir accès ou communication de tout ou partie des données, l'obligation de journaliser les données, et quelles sont les autorités de protection des données compétentes.

Par ailleurs, dans une optique de cohérence, le législateur a choisi pour les autres règles en matière de protection des données (obligation des responsables du traitement, choix d'un sous-traitant, droits des personnes concernées, ...) de se raccrocher par analogie au titre 3, sous-titre 4 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, qui est dédié aux traitements de données à caractère

¹⁹ Ceci a également pour conséquence de modifier le statut du personnel qui sera affecté à la gestion de la banque de données commune puisque celui-ci ne tombera plus sous le régime de l'article 184 de la Constitution.

(artikel 7, § 1, van het voorontwerp), de koppeling aan andere gegevensbanken waaronder authentieke gegevensbronnen (artikel 7 van het voorontwerp), het begrip "inbreuken op de beveiliging" (artikel 13 van het voorontwerp), de omstandigheid dat de dreigingsevaluatie wordt meegedeeld aan de partnerdiensten bij de uitoefening van het vraagrecht (artikel 23 van het voorontwerp), de beschrijving van de inhoud van de evaluatie die moet worden uitgevoerd vóór de mededeling van de informatiekaart aan een derde overheid of instelling (artikel 24, tweede lid, van het voorontwerp), de validering van de dreigingsevaluatie door het OCAD (artikel 27, eerste lid, van het voorontwerp) of nog de oprichting van "lokale task forces" (lees: "lokale taskforces"), afgekort "LTF", waarin veiligheidsprofessionals samen de wenselijkheid onderzoeken van het nemen van maatregelen ten aanzien van een geregistreerde entiteit (artikelen 31 tot 33 van het voorontwerp).

II. — Verwerking van persoonsgegevens

A. Afstemming van de regels inzake gegevensbescherming vervat in het voorontwerp op de regels vervat in de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens'

Eenzijds werkt het voorontwerp een op zichzelf staand dispositief uit ten opzichte van de wet 'op het politieambt'¹⁹, dat ertoe strekt de gemeenschappelijke gegevensbank T.E.R. op te richten, en anderzijds wijzigt het onder meer bepalingen in de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens'.

In de bespreking van de artikelen 4 en 34 wordt daarover het volgende gezegd:

"Dit wetsontwerp regelt de gegevensbeschermingskwes-ties die specifiek zijn voor de verwerking van gegevens in de gemeenschappelijke gegevensbank T.E.R., namelijk welke soorten persoonsgegevens daar worden verwerkt, voor welke doeleinden, hoe lang, wie verantwoordelijk is voor de verwerking, welke autoriteiten de databank moeten voeden, met welke categorieën gegevens, welke categorieën autoriteiten toegang kunnen krijgen tot of mededeling kunnen doen van alle of een deel van de gegevens, de verplichting om de gegevens vast te leggen, en welke gegevensbeschermingsautoriteiten bevoegd zijn.

Voorts heeft de wetgever met het oog op de samenhang ervoor gekozen om de andere regels inzake gegevensbescherming (verplichting van de voor de verwerking verantwoordelijken, keuze van een verwerker, rechten van de betrokkenen, ...) naar analogie te relateren aan titel 3, subtitel 4, van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, die gewijd is aan de verwerking van persoonsgegevens

¹⁹ Dat heeft ook een wijziging tot gevolg van het statuut van het personeel dat zal worden ingezet voor het beheer van de gemeenschappelijke gegevensbank, aangezien dat personeel niet meer onder de regeling van artikel 184 van de Grondwet zal vallen.

personnel réalisés par l'OCAM. Bien que le contexte qui entoure les traitements de données à caractère personnel par l'OCAM au moyen de ses propres systèmes d'informations est fort différent du contexte particulier qui entoure les traitements de données à caractère personnel réalisés au sein de la banque de données commune T.E.R., nous retrouvons dans les deux cas une mutualisation de données à caractère personnel et d'informations provenant de responsables du traitement qui ne sont pas tous soumis aux mêmes obligations en matière de protection des données à caractère personnel. Il est impératif, pour garantir la plus grande sécurité juridique possible, mais également en termes de lisibilité pour les personnes concernées – et par conséquent, faciliter l'exercice de leurs droits – de définir un régime commun à ces traitements”.

Pour la protection des personnes physiques à l'égard du traitement des données à caractère personnel par la banque de données communes T.E.R., il résulte de ce qui précède que le dispositif autonome créé par l'avant-projet et les articles 138 à 167 de la loi du 30 juillet 2018 ‘relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel’, tels qu'ils sont modifiés par l'avant-projet – et sous réserve des dérogations prévues par celui-ci –, s'appliquent complémentarément afin d'énoncer l'ensemble des règles en matière de traitement des données à caractère personnel pour les traitements ainsi concernés au regard du droit au respect de la vie privée et de l'admissibilité des ingérences dans l'exercice de ce droit en la matière.

Or, on constate notamment ce qui suit:

– l'article 4, alinéa 2, énonce que, par dérogation à l'article 162 de la loi du 30 juillet 2018 ‘relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel’, la consultation des données à caractère personnel et des informations enregistrées dans la banque de données commune T.E.R. pour un traitement ultérieur à des fins historiques, scientifiques ou statistiques est autorisée par le responsable opérationnel après concertation avec les services de base, alors que l'article 46 de l'avant-projet entend compléter l'article 162 précité par un alinéa comportant une dérogation identique²⁰;

– l'article 7, § 2, alinéa 5, est inutile dès lors qu'il est déjà prévu, à l'article 4, alinéa 1^{er}, de l'avant-projet que les règles relatives à la protection des données et aux droits de la personne concernée sont celles visées au titre 3, sous-titre 4, de la loi précitée du 30 juillet 2018, qui comprend les articles 162 à 167, lesquels concernent le traitement de données à caractère personnel à des fins historiques, scientifiques ou statistiques;

– l'article 29, § 3, 4^o, et § 4, paraphrase inutilement l'article 157, § 3, alinéa 2, et § 4, de la même loi du 30 juillet 2018.

Interrogée à ce propos, la déléguée du ministre a répondu ce qui suit:

²⁰ Voir aussi l'observation formulée sous l'article 46.

door het OCAD. Hoewel de context rond de verwerkingen van persoonsgegevens door het OCAD door middel van de eigen informatiesystemen ervan sterk verschilt van de specifieke context rond de verwerkingen van persoonsgegevens in de gemeenschappelijke gegevensbank T.E.R., vinden we in beide gevallen een mutualisering terug van persoonsgegevens en informatie afkomstig van verwerkingsverantwoordelijken die niet allemaal onderworpen zijn aan dezelfde verplichtingen inzake bescherming van persoonsgegevens. Om een zo groot mogelijke rechtszekerheid te waarborgen maar ook op het stuk van leesbaarheid voor de betrokken personen – en bijgevolg om de uitoefening van hun rechten te vergemakkelijken, moet een gemeenschappelijke regeling voor die verwerkingen worden bepaald.”

Wat betreft de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door de gemeenschappelijke gegevensbank T.E.R., blijkt uit het voorgaande dat het op zichzelf staande dispositief dat in het voorontwerp wordt ontworpen en de artikelen 138 tot 167 van de wet van 30 juli 2018 ‘betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens’ zoals ze bij het voorontwerp worden gewijzigd – en onder voorbehoud van de afwijkingen waarin het voorontwerp voorziet – aanvullend van toepassing zijn, en zo alle regels in verband met de verwerking van persoonsgegevens bevatten die voor de betreffende verwerkingen gelden in het licht van het recht op eerbiediging van het privéleven en de toelaatbaarheid van inmengingen in de uitoefening van dat recht in deze aangelegenheid.

Men stelt echter met name het volgende vast:

– artikel 4, tweede lid, stelt dat, in afwijking van artikel 162 van de wet van 30 juli 2018 ‘betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens’, de raadpleging van de persoonsgegevens en de informatie geregistreerd in de gemeenschappelijke gegevensbank T.E.R. voor een verdere verwerking voor historische, wetenschappelijke of statistische doeleinden, wordt toegestaan door de operationeel verantwoordelijke na overleg met de basisdiensten; artikel 46 van het voorontwerp strekt er echter toe het voornoemde artikel 162 aan te vullen met een lid dat een identieke afwijking bevat;²⁰

– artikel 7, § 2, vijfde lid, is overbodig aangezien in artikel 4, eerste lid, van het voorontwerp al wordt bepaald dat de regels inzake de gegevensbescherming en inzake de rechten van de betrokken persoon die zijn welke worden bedoeld in titel 3, ondertitel 4, van de voornoemde wet van 30 juli 2018, waartoe de artikelen 162 tot 167 behoren, die betrekking hebben op de verwerking van persoonsgegevens voor historische, wetenschappelijke of statistische doeleinden;

– artikel 29, § 3, 4^o, en § 4, is een overbodige parafrase van artikel 157, § 3, tweede lid, en § 4, van dezelfde wet van 30 juli 2018.

Op een vraag daarover heeft de gemachtigde van de minister het volgende geantwoord:

²⁰ Zie ook de opmerking bij artikel 46.

“Il faut bien entendu éviter de répéter la [loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel dans la loi [relative à la banque de données commune]. Les articles du projet de loi [...] vont être comparés avec le titre III de la loi sur la protection des données pour s'assurer qu'il n'y a pas de double emploi”.

L'avant-projet sera revu en ce sens.

B. Les principes de légalité et de proportionnalité liés à un traitement de données à caractère personnel.

1. Le fonctionnement de la banque de données commune T.E.R. implique un traitement de données à caractère personnel, qui doit être examiné au regard des principes de légalité et de proportionnalité se déduisant, en ce qui concerne le droit au respect de la vie privée, de l'article 22 de la Constitution et de l'article 8 de la Convention européenne des droits de l'homme.

B.1. Le principe de légalité

2.1. Sur le principe de légalité en la matière, dans son avis 70.542/AG donné le 24 décembre 2021 sur un avant-projet de loi 'relatif à la vaccination obligatoire des professionnels des soins de santé contre la COVID-19', la section de législation a observé ce qui suit:

“62. Pour être admissible au regard des dispositions précitées, l'ingérence dans l'exercice du droit au respect de la vie privée doit être définie en des termes clairs et suffisamment précis qui permettent d'appréhender de manière prévisible les hypothèses dans lesquelles le législateur autorise une pareille ingérence. Toute ingérence dans le droit au respect de la vie privée doit, en outre, reposer sur une justification objective et raisonnable et, par conséquent, être proportionnée aux buts poursuivis par le législateur²¹. Si les ingérences prévues par le projet à l'examen poursuivent un objectif légitime (voy. *supra*, nos 43 à 45), il convient de vérifier le respect des exigences de légalité (i), de pertinence et de proportionnalité (ii).

²¹ Note de bas de page n° 122 de l'avis cité: Avis 63.192/2 donné le 19 avril 2018 sur un avant-projet devenu la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel' (*Doc. parl.*, Chambre, 2017-2018, n° 54-3126/001, pp. 402 à 456; <http://www.raadvst-consetat.be/dbx/avis/63192.pdf>; avis 63.202/2 donné le 26 avril 2018 sur un avant-projet devenu la loi du 5 septembre 2018 'instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE' (*Doc. parl.*, Chambre, 2017-2018, n° 54-3185/001, pp. 120 à 145, <http://www.raadvst-consetat.be/dbx/avis/63202.pdf>).

“Il faut bien entendu éviter de répéter la [loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel dans la loi [relative à la banque de données commune]. Les articles du projet de loi (...) vont être comparés avec le titre III de la loi sur la protection des données pour s'assurer qu'il n'y a pas de double emploi.”

Het voorontwerp moet in die zin worden herzien.

B. Het legaliteitsbeginsel en het evenredigheidsbeginsel in verband met een verwerking van persoonsgegevens

1. De werkwijze van de gemeenschappelijke gegevensbank T.E.R. impliceert een verwerking van persoonsgegevens. Deze dient te worden onderzocht in het licht van het legaliteitsbeginsel en het evenredigheidsbeginsel, die, wat het recht op eerbiediging van het privéleven betreft, voortvloeien uit artikel 22 van de Grondwet en uit artikel 8 van het Europees Verdrag voor de rechten van de mens.

B.1. Legaliteitsbeginsel

2.1. Over het legaliteitsbeginsel ter zake heeft de afdeling Wetgeving in haar advies 70.542/AV van 24 december 2021 over een voorontwerp van wet 'betreffende de verplichte vaccinatie tegen COVID-19 van gezondheidszorgbeoefenaars' het volgende opgemerkt:

“62. Om in het licht van de voornoemde bepalingen aanvaardbaar te zijn, moet de inmenging in het recht op eerbiediging van het privéleven geformuleerd worden in duidelijke en voldoende nauwkeurige bewoordingen die het mogelijk maken te voorzien in welke gevallen de wetgever een dergelijke inmenging toestaat. Elke inmenging in het recht op eerbiediging van het privéleven moet bovendien steunen op een objectieve en redelijke verantwoording en bijgevolg evenredig zijn met de door de wetgever nagestreefde doelstellingen.²¹ Hoewel met de inmengingen waarin voorliggend voorontwerp van wet voorziet een legitiem doel nagestreefd wordt (cf. *supra*, opmerkingen 43 tot 45), dient nagegaan te worden of aan de vereisten van legaliteit (i), relevantie en proportionaliteit (ii) voldaan wordt.

²¹ Voetnoot 122 van het geciteerde advies: Adv.RvS 63.192/2 van 19 april 2018 over een voorontwerp dat heeft geleid tot de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens', *Parl. St.* Kamer 2017-18, nr. 54-3126/001, 402 tot 456, <http://www.raadvst-consetat.be/dbx/adviezen/63192.pdf>; adv.RvS 63.202/2 van 26 april 2018 verstrekt over een voorontwerp dat heeft geleid tot de wet van 5 september 2018 'tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG', *Parl. St.* Kamer 2017-18, nr. 54-3185/001, 120 tot 145, <http://www.raadvstconsetat.be/dbx/adviezen/63202.pdf>.

i) La légalité

63. Sur le principe de légalité inhérent au droit au respect de la vie privée garanti par l'article 22 de la Constitution, l'assemblée générale de la section de législation a exposé ce qui suit dans son avis 68.936/AG [donné le 7 avril 2021 sur un avant-projet devenu la loi du 14 août 2021 'relative aux mesures de police administrative lors d'une situation d'urgence épidémique'²²]:

'Conformément à l'article 22 de la Constitution, tout traitement de données à caractère personnel et, plus généralement, toute atteinte au droit à la vie privée, sont soumis au respect d'un principe de légalité formelle²³.

En réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée, l'article 22 de la Constitution garantit à tout citoyen qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue. Une délégation à un autre pouvoir n'est toutefois pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les 'éléments essentiels' sont fixés préalablement par le législateur²⁴.

Par conséquent, les 'éléments essentiels' des traitements de données à caractère personnel doivent être fixés dans la loi elle-même. À cet égard, la section de législation considère que, quelle que soit la matière concernée, constituent, en principe, des 'éléments essentiels' les éléments suivants: 1°) les catégories de données traitées; 2°) les catégories de personnes concernées; 3°) la finalité poursuivie par le traitement; 4°) les catégories de personnes ayant accès aux données traitées; et 5°) le délai maximal de conservation des données²⁵²⁶.

La Cour constitutionnelle s'est prononcée dans le même sens dans ses arrêts n° 33/2022 du 10 mars 2022²⁷ et n° 110/2022 du 22 septembre 2022²⁸.

²² *Doc. parl.*, Chambre, 2021-2022, n° 55-2533/001, pp. 57 et s.

²³ *Note de bas de page n° 123 de l'avis cité*: Note de bas de page n° 174 de l'avis cité: Déjà invoqué plus avant, numéros 70 et s.

²⁴ *Note de bas de page n° 124 de l'avis cité*: Note de bas de page n° 175 de l'avis cité: Jurisprudence constante de la Cour constitutionnelle: voir notamment C.C., 18 mars 2010, n° 29/2010, B.16.1; C.C., 20 février 2020, n° 27/2020, B.17.

²⁵ *Note de bas de page n° 125 de l'avis cité*: Avis 68.936/AG précité, observation n° 101 (*Doc. parl.*, Chambre, 2020-2021, n° 55-1951/001, p. 119; <http://www.raadvst-consetat.be/dbx/avis/68936.pdf>).

²⁶ Avis 70.542/AG donné le 24 décembre 2021 sur un avant-projet de loi 'relatif à la vaccination obligatoire des professionnels des soins de santé contre la COVID-19', observations n°s 62 et 63 (*Doc. parl.*, Chambre, 2021-2022, n° 55-2533/001, pp. 98 et 99).

²⁷ C.C., n° 33/2022, 10 mars 2022, B.13.1.

²⁸ C.C., n° 110/2022, 22 septembre 2022, B.11.2.

i) Legaliteit

63. Met betrekking tot het legaliteitsbeginsel, dat onlosmakelijk verbonden is met het recht op eerbiediging van het privéleven gewaarborgd in artikel 22 van de Grondwet, heeft de algemene vergadering van de afdeling Wetgeving het volgende uiteengezet in voornoemd advies 68.936/AV [van 7 april 2021 over een voorontwerp dat geleid heeft tot de wet van 14 augustus 2021 'betreffende de maatregelen van bestuurlijke politie tijdens een epidemische noodsituatie'²²]:

'Krachtens artikel 22 van de Grondwet geldt voor elke verwerking van persoonsgegevens en, meer in het algemeen, voor elke schending van het recht op het privéleven, dat het formeel legaliteitsbeginsel²³ dient te worden nageleefd.

Doordat artikel 22 van de Grondwet aan de bevoegde wetgever de bevoegdheid voorbehoudt om vast te stellen in welke gevallen en onder welke voorwaarden afbreuk kan worden gedaan aan het recht op eerbiediging van het privéleven, waarborgt het aan elke burger dat geen enkele inmenging in dat recht kan plaatsvinden dan krachtens regels die zijn aangenomen door een democratisch verkozen beraadslagende vergadering. Een delegatie aan een andere macht is evenwel niet in strijd met het wettelijkheidsbeginsel voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de 'essentiële elementen' voorafgaandelijk door de wetgever vastgesteld zijn.²⁴

Bijgevolg moeten de 'essentiële elementen' van de verwerking van persoonsgegevens in de wet zelf worden vastgelegd. In dat verband is de afdeling Wetgeving van oordeel dat ongeacht de aard van de betrokken aangelegenheid, de volgende elementen in beginsel 'essentiële elementen' uitmaken: 1°) de categorie van verwerkte gegevens; 2°) de categorie van betrokken personen; 3°) de met de verwerking nagestreefde doelstelling; 4°) de categorie van personen die toegang hebben tot de verwerkte gegevens; en 5°) de maximumtermijn voor het bewaren van de gegevens.²⁵²⁶

Het Grondwettelijk Hof heeft zich in dezelfde zin uitgesproken in zijn arresten nr. 33/2022 van 10 maart 2022²⁷ en nr. 110/2022 van 22 september 2022.²⁸

²² *Parl. St. Kamer* 2021-22, nr. 55-2533/001, 57 e.v.

²³ *Voetnoot 123 van het geciteerde advies*: Voetnoot 174 van het geciteerde advies: Wat dit beginsel betreft, zie *supra* randnummers 70 en v.

²⁴ *Voetnoot 124 van het geciteerde advies*: Voetnoot 175 van het geciteerde advies: Vaste rechtspraak van het Grondwettelijk Hof: zie inzonderheid GwH 18 maart 2010, nr. 29/2010, B.16.1; GwH 20 februari 2020, nr. 27/2020, B.17.

²⁵ *Voetnoot 125 van het geciteerde advies*: Voornoemd adv. RvS 68.936/AV, opmerking 101 (*Parl. St. Kamer* 2020-21, nr. 55-1951/001, 119; <http://www.raadvst-consetat.be/dbx/avis/68936.pdf>).

²⁶ Advies 70.542/AV van 24 december 2021 over een voorontwerp van wet 'betreffende de verplichte vaccinatie tegen COVID-19 van gezondheidszorgbeoefenaars', opmerkingen 62 en 63 (*Parl. St. Kamer* 2021-22, nr. 55-2533/001, 98 en 99).

²⁷ GwH 10 maart 2022, nr. 33/2022, B.13.1.

²⁸ GwH 22 september 2022, nr. 110/2022, B.11.2.

2.2. Il y a lieu de constater que plusieurs éléments essentiels relatifs au traitement des données dans le cadre de la banque de données commune T.E.R. sont effectivement énoncés dans le texte en projet:

– les catégories de données à caractère personnel qui y sont traitées (article 6, § 2) (sous réserve des critiques formulées dans les observations n^{os} 2.5 à 2.7, ci-dessous);

– les finalités poursuivies (article 5, alinéa 2) (sous réserve de la critique formulée dans l'observation n^o 2.8, ci-dessous);

– le délai de conservation (article 7, §§ 1^{er} et 2);

– les catégories de personnes qui ont accès aux données traitées (articles 15, 16, 17 et 21 à 28).

Bien qu'ils ne constituent pas des éléments essentiels au sens de la jurisprudence et de la jurisprudence précitées, d'autres éléments sont par ailleurs également déterminés par l'avant-projet:

– le responsable du traitement (article 5, alinéa 1^{er});

– la journalisation des données (article 8);

– les règles relatives au délégué à la protection des données et à la responsabilité de la qualité des données à caractère personnel, ainsi que des informations enregistrées (articles 29 et 30).

2.3. Le dispositif en projet appelle toutefois un certain nombre de critiques au regard du principe de légalité, exposées ci-dessous:

a) En ce qui concerne les catégories de personnes concernées par le traitement de données à caractère personnel

2.4. Les articles 2, 4^o, et 6, § 2, alinéa 4, de l'avant-projet chargent le Roi de déterminer, par arrêté délibéré en Conseil des ministres, les catégories d'"entités" à propos desquelles les données visées à l'alinéa 1^{er} de cette dernière disposition sont traitées, tandis que l'article 6, § 1^{er}, semble donner une autre portée à la catégorie de personnes dont les données à caractère personnel seront traitées dans la banque de données commune T.E.R. lorsqu'il y vise les "personnes, [...] groupements, [...] organisations [ou] phénomènes" et non plus la notion d'"entités", ce qui prête à confusion.

Interrogée à ce sujet, la déléguée du ministre a précisé que les catégories de personnes dont les données à caractère personnel pourront être traitées concernent cinq catégories d'entités, qui seront prévues dans l'arrêté royal à adopter en exécution de l'article 6, § 2, alinéa 4, de l'avant-projet, à savoir:

1^o les *foreign terrorist fighters*;

2.2. Er dient te worden vastgesteld dat de ontworpen tekst inderdaad verschillende essentiële elementen vermeldt betreffende de gegevensverwerking in het kader van de gemeenschappelijke gegevensbank T.E.R.:

– de categorieën van persoonsgegevens die daarin worden verwerkt (artikel 6, § 2) (onder voorbehoud van de kritiek die in de opmerkingen 2.5 tot 2.7, *infra*, wordt geformuleerd);

– de nagestreefde doeleinden (artikel 5, tweede lid) (onder voorbehoud van de kritiek die in opmerking 2.8, *infra*, wordt geformuleerd);

– de bewaartermijn (artikel 7, §§ 1 en 2);

– de categorieën van personen die toegang hebben tot de verwerkte gegevens (artikelen 15, 16, 17 en 21 tot 28).

Het voorontwerp stelt voorts andere gegevens vast, hoewel die geen essentiële elementen zijn in de zin van de bovenvermelde adviespraktijk en rechtspraak:

– de verantwoordelijke voor de verwerking (artikel 5, eerste lid);

– de logbestanden van de gegevens (artikel 8);

– de regels betreffende de functionaris voor gegevensbescherming en betreffende de verantwoordelijkheid voor de kwaliteit van de persoonsgegevens en voor de geregistreerde informatie (artikelen 29 en 30).

2.3. Ten aanzien van het legaliteitsbeginsel geeft het ontworpen dispositief evenwel aanleiding tot de volgende punten van kritiek:

a) *Wat betreft de categorieën van personen wier persoonsgegevens worden verwerkt*

2.4. De artikelen 2, 4^o, en 6, § 2, vierde lid, van het voorontwerp belasten de Koning ermee bij een besluit vastgesteld na overleg in de Ministerraad de categorieën van "entiteiten" te bepalen waarvan de in het eerste lid van die laatstgenoemde bepaling vermelde gegevens worden verwerkt. Artikel 6, § 1, verwijst dan weer naar "personen, groeperingen, organisaties en fenomenen" in plaats van naar "entiteiten" en lijkt op die manier een andere inhoud te geven aan de categorie van personen wier persoonsgegevens in de gemeenschappelijke gegevensbank T.E.R. zullen worden verwerkt. Dat creëert onduidelijkheid.

Naar aanleiding van een vraag daarover heeft de gemachtigde van de minister uitgelegd dat de categorieën van personen wier persoonsgegevens mogen worden verwerkt, betrekking hebben op vijf categorieën van entiteiten, die opgesomd zullen worden in het koninklijk besluit dat ter uitvoering van artikel 6, § 2, vierde lid, van het voorontwerp, moet worden vastgesteld, te weten:

1^o de *foreign terrorist fighters*;

2° les *homegrown terrorist fighters*;

3° les extrémistes potentiellement violents;

4° les personnes condamnées pour terrorisme;

5° les propagandistes de haine.

Dans le dernier alinéa du commentaire de l'article 6, on peut lire ce qui suit:

"L'article 6, § 2, alinéa 4, habilite le Roi à déterminer, par arrêté délibéré en Conseil des ministres, les catégories d'entités à propos desquelles les données visées à l'alinéa précédent sont traitées. En effet, ces catégories étant susceptibles d'évoluer en fonction des besoins opérationnels, tactiques ou stratégiques, il est dès lors préférable de les déterminer par arrêté royal. En outre, actuellement, ces catégories sont les suivantes: les '*Foreign Terrorist Fighters*', les '*Homegrown Terrorist Fighters*', les '*Propagandistes de haine*', les '*Extrémistes Potentiellement Violents*', les '*Personnes condamnées pour terrorisme*' et les entités en '*pré-enquête*', c'est-à-dire qui n'entrent pas, au moment de leur enregistrement dans la banque de données commune T.E.R., dans les critères pour être considérées comme *foreign terrorist fighter*, *homegrown terrorist fighter*, extrémiste potentiellement violent ou propagandiste de haine [...]."

Les catégories d'"entités" constituent un élément central, et donc essentiel, du dispositif en projet, qui doit en conséquence être fixé par le législateur.

La circonstance que ces catégories d'"entités" sont susceptibles d'évoluer en fonction des besoins opérationnels, tactiques ou stratégiques ne peut dès lors justifier en soi une habilitation au Roi sur un point aussi essentiel, d'autant moins que le nombre de catégories d'entités est non seulement fixé mais qu'il est également limité.

Par ailleurs, ainsi que cela ressort du commentaire de l'article 6, l'auteur de l'avant-projet entend inclure dans le champ d'application des catégories de personnes dont les données à caractère personnel seront traitées, les "entités" en "pré-enquête". Le même commentaire précise à cet égard que le but de la période de pré-enquête est le suivant:

"[...] Pour les entités en 'pré-enquête', il faut préciser que le but de cette période de 'pré-enquête' est de permettre la collecte temporaire (au maximum six mois) mais centralisées dans un seul système de traitement de l'information de données et d'informations qui pourront ou non justifier une validation de l'entité concernée en tant que *foreign terrorist fighter*, *homegrown terrorist fighter*, extrémiste potentiellement violent ou propagandiste de haine ('phase d'enrichissement'). À l'issue de cette période, sur la base des informations/renseignements disponibles, l'OCAM évaluera si les critères légaux sont rencontrés ou non. S'ils ne sont pas rencontrés, l'entité en pré-enquête sera automatiquement archivée. Il s'agit donc d'une situation temporaire à l'issue de laquelle cette entité sera ou non maintenue dans la banque de données commune T.E.R.."

2° de *homegrown terrorist fighters*;

3° de potentiellement gewelddadige extremisten;

4° de terrorismeveroordeelden;

5° de haatpropagandisten.

In de laatste alinea van de bespreking van artikel 6 staat het volgende te lezen:

"Artikel 6, § 2, vierde lid, machtigt de Koning ertoe, bij een in Ministerraad overlegd besluit, de categorieën van entiteiten te bepalen waarvan de in het vorige lid bedoelde gegevens verwerkt worden. Aangezien die categorieën kunnen evolueren op grond van de operationele, tactische of strategische behoeften, is het derhalve wenselijk om deze bij koninklijk besluit te bepalen. Momenteel gaat het om de volgende categorieën: de '*Foreign Terrorist Fighters*', de '*Homegrown Terrorist Fighters*', de '*Haatpropagandisten*', de '*Potentieel Gewelddadige Extremisten*', de '*Terrorismeveroordeelden*' en de entiteiten in 'vooronderzoek', d.w.z. die, op het ogenblik van hun registratie in de gegevensbank T.E.R., niet beantwoorden aan de criteria om als een *foreign terrorist fighter*, *homegrown terrorist fighter*, potentieel gewelddadige extremist of haatpropagandist beschouwd te worden (...)."

De categorieën van "entiteiten" vormen een kernaspect en dus een essentieel element van het ontworpen dispositief, dat bijgevolg door de wetgever dient te worden vastgesteld.

De omstandigheid dat die categorieën van "entiteiten" kunnen evolueren in functie van de operationele, tactische of strategische behoeften, kan op zich niet rechtvaardigen dat de Koning op zo'n essentieel punt een machtiging wordt verleend, des te minder daar het aantal categorieën van entiteiten niet enkel wordt vastgesteld maar ook wordt beperkt.

Voorts wil de steller van het voorontwerp, zoals uit de bespreking van artikel 6 blijkt, de "entiteiten in 'vooronderzoek'" opnemen in het toepassingsgebied van de categorieën van personen wier persoonsgegevens worden verwerkt. In dat verband wordt in diezelfde bespreking gepreciseerd wat het doel is van de periode van vooronderzoek:

"(...) Voor de entiteiten in 'vooronderzoek' moet worden gespecificeerd dat het doel van die periode van 'vooronderzoek' namelijk is om tijdelijk (maximaal zes maanden) maar gecentraliseerd in één enkel informatieverwerkingssysteem gegevens en informatie te kunnen inzamelen die al dan niet een validering van de betrokken entiteit als *foreign terrorist fighter*, *homegrown terrorist fighter*, potentieel gewelddadige extremist of haatpropagandist zullen onderbouwen ('verrijkingsfase'). Na afloop ervan zal het OCAD, op basis van de beschikbare informatie/inlichtingen, evalueren of de wettelijke criteria al dan niet vervuld zijn. Indien deze niet vervuld zijn, zal de entiteit in vooronderzoek automatisch gearchiveerd worden. Het betreft bijgevolg een tijdelijke situatie. Na afloop ervan zal deze entiteit al dan niet in de gemeenschappelijke gegevensbank T.E.R. geregistreerd blijven."

Or le dispositif en projet n'apporte aucun élément quant aux contours de la notion de "pré-enquête" ni au régime juridique qui devrait s'appliquer aux "entités" relevant de cette catégorie.

Pour rappel, il faut pouvoir appréhender de manière prévisible les différentes hypothèses dans lesquelles le législateur autorise une ingérence dans le droit au respect de la vie privée en fixant dans l'avant-projet les catégories de personnes, qualifiées d'"entités" par l'avant-projet, pour lesquelles il est admissible de rassembler les différentes catégories de données à caractère personnel dans la banque de données commune T.E.R.

Les articles 2, 4° et 6, §§ 1^{er} et 2, alinéa 4, doivent être revus en ce sens.

Le dispositif sera également complété afin de préciser le régime juridique applicable à la catégorie des "entités" en "pré-enquête", dont la notion sera par ailleurs définie.

2.5. L'article 6, § 2, alinéa 1^{er}, 1°, 1), b), de l'avant-projet contient une habilitation au Roi en ce qui concerne les données relatives aux enfants mineurs biologiques ou adoptés d'une "entité" personne physique enregistrée dans la banque de données commune T.E.R.

Le commentaire de cette disposition ajoute une information importante puisqu'il précise que cette disposition concerne uniquement les enfants mineurs qui séjournent ou ont séjournés en zone de conflit djihadiste.

Interrogée sur ce point, la déléguée du ministre a répondu qu'à l'heure actuelle c'est en effet la seule hypothèse envisagée puisque, ainsi qu'elle l'a expliqué,

"[...] dans le but de les identifier de manière certaine, les données d'identification visées des enfants mineurs des deux catégories d'entités suivantes, seront enregistrées dans la [banque de données commune] T.E.R.:

1° les *foreigns terrorist fighters* qui se sont rendus dans une zone de conflit djihadiste (FTF catégorie 1);

2° les *foreigns terrorist fighters* qui sont en route vers la Belgique ou sont revenus en Belgique après s'être rendus dans une zone de conflit djihadiste (FTF catégorie 3)".

Dès lors qu'il y a lieu de définir le plus précisément possible les hypothèses dans lesquelles un traitement de données à caractère personnel concernant des enfants mineurs peut être réalisé dans une banque de données telle que la banque de données commune T.E.R., ces précisions relatives à cette catégorie de données doivent figurer dans le dispositif en projet.

L'article 6, § 2, alinéa 1^{er}, 1°, 1), b), sera revu en conséquence.

b) En ce qui concerne les catégories de données à caractère personnel traitées

In het ontworpen dispositief wordt het begrip "vooronderzoek" echter op geen enkele wijze afgebakend, en wordt evenmin iets bepaald in verband met de juridische regeling die zou gelden voor de "entiteiten" die onder die categorie vallen.

Er wordt aan herinnerd dat men steeds duidelijk de verschillende gevallen moet kunnen voorzien waarin de wetgever een inmenging in het recht op eerbiediging van het privéleven toestaat. Daartoe dient het voorontwerp te bepalen voor welke categorieën van personen, die in het voorontwerp "entiteiten" worden genoemd, kan worden aanvaard dat de verschillende categorieën van persoonsgegevens in de gemeenschappelijke gegevensbank T.E.R. worden verzameld.

De artikelen 2, 4°, en 6, §§ 1 en 2, vierde lid, moeten in die zin worden herzien.

Ook moet in het dispositief aanvullend worden gepreciseerd welke juridische regeling van toepassing is op de categorie "entiteiten" in "vooronderzoek", een begrip dat overigens nog dient te worden gedefinieerd.

2.5. Artikel 6, § 2, eerste lid, 1°, 1), b), van het voorontwerp verleent een machtiging aan de Koning voor wat betreft de gegevens betreffende de biologische of geadopteerde minderjarige kinderen van een natuurlijke persoon-"entiteit" die in de gemeenschappelijke gegevensbank T.E.R. is geregistreerd.

De bespreking van die bepaling bevat belangrijke aanvullende informatie: ze stelt dat die bepaling enkel betrekking heeft op minderjarige kinderen die in een jihadistisch conflictgebied verblijven of hebben verbleven.

Op een vraag daarover heeft de gemachtigde van de minister geantwoord dat dat momenteel inderdaad het enige geval is dat wordt beoogd. Ze geeft daarvoor de volgende uitleg:

"(...) dans le but de les identifier de manière certaine, les données d'identification visées des enfants mineurs des deux catégories d'entités suivantes, seront enregistrées dans la [banque de données commune] T.E.R.:

1° les *foreigns terrorist fighters* qui se sont rendus dans une zone de conflit djihadiste (FTF catégorie 1);

2° les *foreigns terrorist fighters* qui sont en route vers la Belgique ou sont revenus en Belgique après s'être rendus dans une zone de conflit djihadiste (FTF catégorie 3)."

Aangezien de gevallen waarin persoonsgegevens van minderjarige kinderen mogen worden verwerkt in een gegevensbank zoals de gemeenschappelijke gegevensbank T.E.R., zo nauwkeurig mogelijk moeten worden omschreven, moeten die preciseringen met betrekking tot deze categorie van gegevens in het ontworpen dispositief worden opgenomen.

Artikel 6, § 2, eerste lid, 1°, 1°, b), moet dienovereenkomstig worden herzien.

b) Wat betreft de categorieën van verwerkte persoonsgegevens

2.6. L'article 2, 4°, de l'avant-projet définit la notion d'"entité" comme étant

"toute personne physique majeure ou mineure de plus de douze ans ou toute personne morale, association de fait, ainsi que l'ensemble des moyens utilisés, déterminés par le Roi [...]".

Il est précisé dans le commentaire de la disposition qu'il s'agit de viser

"non seulement les personnes physiques et morales mais aussi les moyens de transport, ou les numéros de téléphone/compte utilisés".

On peut encore y lire ce qui suit à ce sujet:

"Le concept d'entité, reprend également, outre toute personne physique ou morale ou association de fait, les moyens utilisés. Ces moyens devant être entendus comme vecteurs de radicalisation. Il est parfois difficile au début d'une enquête d'identifier l'entité en tant que personne physique ou morale ou association de fait. Souvent, il sera plus aisé d'identifier le moyen utilisé (site Internet, radio, presse, etc.). Dans ce cas, les moyens doivent être repris dans la banque de données commune T.E.R. Le suivi des moyens utilisés repris dans la banque de données permet alors de prendre, le cas échéant, les mesures adéquates".

L'ensemble du dispositif est conçu en manière telle, que lorsqu'il vise la notion d'"entité", celle-ci semble couvrir des personnes physiques, morales ou des associations de fait dont les données peuvent faire l'objet d'un traitement dans la banque de données commune T.E.R. Lorsque ces données portent sur des personnes physiques, il s'agit de données à caractère personnel au sens de l'article 4, point 1), du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 'relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)' (dans la suite de l'avis: "le RGPD") et de l'article 3, point 1), de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 'relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de

2.6. In artikel 2, 4°, van het voorontwerp wordt het begrip "entiteit" gedefinieerd als

"elke meerderjarige natuurlijke persoon of minderjarige natuurlijke persoon ouder dan twaalf jaar of elke rechtspersoon, feitelijke vereniging alsook alle aangewende middelen, bepaald door de Koning (...)".

In de bespreking van de bepaling wordt nader bepaald dat die term

"niet alleen [doelt] op natuurlijke en rechtspersonen, maar ook op vervoersmiddelen of gebruikte telefoon-/rekeningnummers."

Daarin staat in dat verband nog het volgende te lezen:

"Het begrip 'entiteit' herneemt, behalve elke natuurlijke persoon of rechtspersoon of feitelijke vereniging, ook de middelen die aangewend worden. Deze middelen moeten worden opgevat als vectoren van radicalisering. Het is bij het begin van een onderzoek echter soms moeilijk om de entiteit te identificeren als een natuurlijke persoon, een rechtspersoon of als feitelijke vereniging. Het identificeren van het gebruikte middel (website, radio, pers, ...) is vaak eenvoudiger. In dit geval moeten de middelen zelf opgenomen worden in de gemeenschappelijke gegevensbank T.E.R. De opvolging van de aangewende middelen hernomen in de gegevensbank laat toe om desgewenst de gepaste maatregelen te nemen."

Het volledige dispositief is aldus opgevat dat verwijzingen naar het begrip "entiteit" lijken te slaan op natuurlijke personen, rechtspersonen of feitelijke verenigingen waarvan de gegevens in de gemeenschappelijke gegevensbank T.E.R. kunnen worden verwerkt. Wanneer die gegevens betrekking hebben op natuurlijke personen, gaat het om persoonsgegevens in de zin van artikel 4, punt 1), van verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 'betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)' (verderop in het advies: "de AVG") en in de zin van artikel 3, punt 1), van richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 'betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en

sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil^{29,30}.

Or, lorsqu'il entend étendre la définition d'"entité" à celle des "moyens utilisés", il s'agit davantage de viser des catégories de données que des catégories de personnes ou d'associations en tant que telles. Compte tenu de ce constat, la notion de "moyens utilisés" trouverait mieux sa place dans l'article 6 de l'avant-projet, où elle serait alors précisée, au même titre que le sont les autres catégories de données qui y sont déjà visées et compte tenu des particularités qui entourent cette notion, ainsi que cela ressort du commentaire de la disposition.

En conséquence, les signe et mots "ainsi que l'ensemble des moyens utilisés," seront omis de la définition de la notion d'"entité" telle qu'elle figure à l'article 2, 4°, de l'avant-projet; le terme "déterminés" sera également remplacé par le mot "déterminées" dans la version française de l'avant-projet.

2.7. L'habilitation conférée au Roi par l'article 9, § 1^{er}, alinéa 2, de l'avant-projet est rédigée en des termes trop larges en ce qu'elle prévoit, sans en définir les éléments essentiels, une extension du contenu de la banque de données commune T.E.R. aux informations provenant d'autres banques

²⁹ Cette directive a été transposée par le titre 2 ("De la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces") de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel', ainsi que le confirme l'article 25 de cette loi.

Aux termes de son article premier, paragraphe 1, "[l]a [...] directive [2016/680] établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces" (voir aussi l'article 27 de la loi précitée du 30 juillet 2018). Certains des services de base et des services partenaires susceptibles de traiter des données à caractère personnel visées par l'avant-projet tombent dans le champ d'application de l'avant-projet, compte tenu également des finalités de ces traitements telles qu'elles sont énoncées par l'article 5, alinéa 2, de l'avant-projet. D'autres de ces services relèvent du RGPD (article 2, paragraphes 1 et 2, d), du RGPD), étant entendu que les services de renseignement et de sécurité sont soumis à un régime particulier (article 3, paragraphe 2, a), de la directive 2016/680; article 2, paragraphe 2, a), du RGPD; voir l'exposé des motifs du projet devenu la loi précitée du 30 juillet 2018, *Doc. parl.*, 2017-2018, Chambre, n° 54-3126/001, notamment, pp. 124 à 126 et 128), organisé par le titre 3, sous-titre 1^{er} ("De la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les services de renseignements et de sécurité"), de la loi précitée du 30 juillet 2018.

³⁰ La définition de la notion de "donnée à caractère personnel", limitant son champ d'application aux "personnes physiques", issue de la définition énoncée par l'article 3, point 1), de la directive, figure également à l'article 26, 1°, de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel'.

betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad^{29,30}.

Wanneer het dispositief de definitie van "entiteit" wil uitbreiden tot de definitie van "aangewende middelen", gaat het echter veeleer om categorieën van gegevens dan om categorieën van personen of van verenigingen als zodanig. Gelet op die vaststelling hoort het begrip "aangewende middelen" veeleer thuis in artikel 6 van het voorontwerp, waar het dan zou moeten worden verduidelijkt, net zoals het geval is met de andere categorieën van gegevens die daar reeds worden vermeld, en rekening houdend met de bijzondere kenmerken van dat begrip, zoals blijkt uit de bespreking van de bepaling.

Bijgevolg moeten de woorden "alsook alle aangewende middelen," worden weggelaten uit de definitie van het begrip "entiteit" zoals die in artikel 2, 4°, van het voorontwerp staat; ook moet het woord "déterminés" in de Franse tekst worden vervangen door het woord "déterminées".

2.7. De machtiging die bij artikel 9, § 1, tweede lid, van het voorontwerp aan de Koning wordt verleend, is te ruim geformuleerd. Zonder dat haar essentiële elementen worden omschreven, bepaalt ze namelijk dat de inhoud van de gemeenschappelijke gegevensbank T.E.R. wordt uitgebreid tot

²⁹ Die richtlijn is omgezet bij titel 2 ("De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door de bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid") van de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens', zoals in artikel 25 van die wet wordt bevestigd.

Luidens artikel 1, lid 1, van richtlijn 2016/680 worden "[b]ij deze richtlijn de regels vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid" (zie eveneens artikel 27 van de voornoemde wet van 30 juli 2018).

Sommige van de basis- en partnerdiensten die de in het voorontwerp bedoelde persoonsgegevens kunnen verwerken, vallen in het toepassingsgebied van het voorontwerp, tevens gelet op de doeleinden van die verwerkingen zoals ze in artikel 5, tweede lid, van het voorontwerp worden vermeld. Andere dergelijke diensten vallen onder de AVG (artikel 2, lid 1 en 2, d), van de AVG), met dien verstande dat voor de inlichtingen- en veiligheidsdiensten een bijzondere regeling geldt (artikel 3, lid 2, a), van richtlijn 2016/680; artikel 2, lid 2, a), van de AVG; zie de memorie van toelichting bij het ontwerp dat heeft geleid tot de voornoemde wet van 30 juli 2018, *Parl. St.* Kamer 2017-18, nr. 54-3126/001, met name 124 tot 126 en 128), waarin titel 3, ondertitel 1 ("De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten"), van de voornoemde wet van 30 juli 2018 voorziet.

³⁰ De definitie van het begrip "persoonsgegeven", die het toepassingsgebied van dat begrip beperkt tot "natuurlijke personen" en die voortkomt uit de definitie vermeld in artikel 3, punt 1), van de richtlijn, staat ook in artikel 26, 1°, van de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens'.

de données via une interconnexion mais sans en fixer les finalités, les catégories de données à caractère personnel interconnectées et les règles relatives à cette interconnexion³¹.

Par conséquent, l'article 9, § 1^{er}, alinéa 2, doit être revu au regard du principe de légalité déduit de l'article 22 de la Constitution et des exigences résultant du RGPD, ainsi que de la directive 2016/680.

c) En ce qui concerne les finalités du traitement de données à caractère personnel

2.8. Le deuxième alinéa que l'article 46 de l'avant-projet tend à insérer à l'article 162 de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel' dispose que toute demande adressée aux Archives de l'État de traitement ultérieur de données à caractère personnel enregistrées dans la banque de données commune T.E.R. à d'autres fins qu'à des fins historiques, scientifiques ou statistiques est refusée "à moins que la finalité soit légitime", sans autre précision.

Or, ainsi qu'il a été rappelé plus haut³², les finalités du traitement de données à caractère personnel constituent un élément essentiel qui doit figurer dans la loi.

Le dispositif sera complété en ce sens, le cas échéant, à la lumière des exemples cités dans le commentaire de la disposition, lequel précise ce qui suit:

"[...] Par exemple, l'article 164 prévoit que si la finalité historique ne peut être obtenue avec des informations pseudonymisées, l'OCAM peut autoriser la consultation des info 'claires' s'il n'y a pas une atteinte disproportionnée à la vie privée (c'est donc un critère qui permet d'apprécier la légitimité de la demande). Par ailleurs, les travaux parlementaires de la loi du 30 juillet 2018 relative à la protection des données précise au sujet de l'article 99, al. 2, que "[p]our répondre à l'avis du Conseil d'État, en page 35, l'alinéa 2 de cet article est reformulé: il est précisé qu'un traitement ultérieur sans finalités historiques, statistiques ou scientifiques est refusé sauf si la finalité est légitime et que la consultation n'est pas susceptible de porter [atteinte] aux intérêts à protéger qui sont visés à l'alinéa premier. Ainsi, il est clair qu'il n'est pas question d'autoriser une finalité – celle-ci devant en elle-même et au préalable être légitime – mais bien une consultation de données dans certains cas. Les critères étant déterminés, il ne s'agit pas d'un pouvoir discrétionnaire. Les modalités sont celles fixées dans le présent chapitre et, le cas échéant, dans d'autres lois (par exemple la loi du 11 décembre 1998)".

informatie die via een koppeling uit andere gegevensbanken afkomstig is, maar er wordt verzuimd de doeleinden van die koppeling, de onderling verbonden categorieën van persoonsgegevens en de regels inzake die koppeling vast te stellen.³¹

Bijgevolg moet artikel 9, § 1, tweede lid, worden herzien in het licht van het legaliteitsbeginsel, dat voortvloeit uit artikel 22 van de Grondwet, en van de vereisten voortvloeiend uit de AVG en uit richtlijn 2016/680.

c) Wat betreft de doeleinden van de verwerking van persoonsgegevens

2.8. Het tweede lid dat bij artikel 46 van het voorontwerp zou worden ingevoegd in artikel 162 van de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens' bepaalt dat elk verzoek aan het Rijksarchief om verdere verwerking van persoonsgegevens die geregistreerd staan in de gemeenschappelijke gegevensbank T.E.R. voor andere dan historische, wetenschappelijke of statistische doeleinden, wordt geweigerd "tenzij het doel legitiem is". Dat laatste wordt niet nader gepreciseerd.

Zoals hierboven in herinnering is gebracht,³² vormen de doeleinden van de verwerking van persoonsgegevens echter een essentieel element dat in de wet moet staan.

Het dispositief moet, in voorkomend geval, in die zin worden aangevuld in het licht van de voorbeelden aangehaald in de bespreking van de bepaling, waarin het volgende wordt gesteld:

"(...) Zo bijvoorbeeld bepaalt artikel 164 dat, indien gepseudonimiseerde gegevens niet toelaten om de historische doeleinden te verwezenlijken, het OCAD de raadpleging van 'clear' info kan toestaan indien dit geen onevenredige afbreuk doet aan het privéleven (het betreft dus een criterium waarmee de legitimiteit van de vraag kan worden beoordeeld). Voorts wordt in het kader van de parlementaire voorbereidingen voor de wet van 30 juli 2018 betreffende de bescherming van de persoonsgegevens in verband met artikel 99, tweede lid, bepaald: 'Om te antwoorden op het advies van de Raad van State (pagina 35) wordt het tweede lid van dit artikel opnieuw geformuleerd: er wordt verduidelijkt dat een verdere verwerking zonder historische, statistische of wetenschappelijke doeleinden geweigerd wordt behalve indien het doeleinde wettelijk is en de raadpleging geen afbreuk kan doen aan de belangen bedoeld in het eerste lid. Zo moet het duidelijk zijn dat er geen sprake is van het toelaten van een doeleinde – deze dient op zich en voorafgaand wettelijk te zijn – maar wel een raadpleging van gegevens in bepaalde gevallen. Aangezien de criteria vastliggen betreft het geen[s]zins een discretionaire bevoegdheid. De modaliteiten zijn deze die zijn vastgelegd in huidig hoofdstuk en, desgevallend, in andere wetten (bijvoorbeeld de wet van 11 december 1998)."

³¹ À comparer avec l'article 9, § 2, qui énumère les données dans les hypothèses d'une interconnexion avec les banques de données sources authentiques.

³² Observation générale n° II, B, 2.1.

³¹ Vergelijk met artikel 9, § 2, waarin wordt opgesomd in welke gevallen een koppeling met de gegevensbanken authentieke bronnen tot stand kan worden gebracht.

³² Algemene opmerking II, B, 2.1.

B.2. *Le principe de proportionnalité*

3. L'exigence de proportionnalité est explicitée par la Cour constitutionnelle dans les termes suivants:

“B.12.1. Une ingérence des pouvoirs publics dans l'exercice du droit au respect de la vie privée doit non seulement reposer sur une disposition législative suffisamment précise mais doit également répondre à un besoin social impérieux dans une société démocratique et être proportionnée au but légitime poursuivi.

Le législateur dispose en la matière d'une marge d'appréciation. Cette marge n'est toutefois pas illimitée: pour qu'une norme soit compatible avec le droit au respect de la vie privée, il faut que le législateur ait ménagé un juste équilibre entre tous les droits et intérêts en cause. Pour juger de cet équilibre, la Cour européenne des droits de l'homme tient compte notamment des dispositions de la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après: la Convention n° 108) et de la recommandation n° R (87) 15 du Comité des ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (ci-après: recommandation n° R (87) 15) (CEDH, 25 février 1997, *Z c. Finlande*, § 95; grande chambre, 12 janvier 2010, *S. et Marper c. Royaume-Uni*, § 103).

B.12.2. Une ingérence dans l'exercice du droit au respect de la vie privée par un traitement de données à caractère personnel doit reposer sur une justification raisonnable et être proportionnée aux buts poursuivis par le législateur. S'agissant du caractère proportionné, la Cour européenne des droits de l'homme tient compte de la présence ou de l'absence de garanties dans la réglementation concernée, destinées à éviter les abus lors du traitement de données à caractère personnel:

‘35. La protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article. Cette nécessité se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières. Le droit interne doit notamment s'assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées. Le droit interne doit aussi contenir des garanties de nature à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs (*S. et Marper c. Royaume-Uni*, précité, § 103, *Gardel c. France*, précité, § 62, CEDH 2009, et *M.K. c. France*, précité, § 35).

B.2. *Evenredigheidsbeginsel*

3. Het Grondwettelijk Hof geeft de volgende expliciete invulling aan het evenredigheidsvereiste:

“B.12.1. Een overheidsinmenging in het recht op eerbiediging van het privéleven dient niet alleen te steunen op een voldoende precieze wettelijke bepaling, maar ook te beantwoorden aan een dwingende maatschappelijke behoefte in een democratische samenleving en evenredig te zijn met de daarmee nagestreefde wettige doelstelling.

De wetgever beschikt ter zake over een appreciatiemarge. Die appreciatiemarge is evenwel niet onbegrensd: opdat een wettelijke regeling verenigbaar is met het recht op eerbiediging van het privéleven, is vereist dat de wetgever een billijk evenwicht heeft gevonden tussen alle rechten en belangen die in het geding zijn. Bij de beoordeling van dat evenwicht houdt het Europees Hof voor de Rechten van de Mens onder meer rekening met de bepalingen van het Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens (hierna: Verdrag nr. 108) en de aanbeveling nr. R (87) 15 van het Comité van ministers aan de verdragsstaten tot regeling van het gebruik van persoonsgegevens in de politiesector (hierna: aanbeveling nr. R (87) 15) (EHRM, 25 februari 1997, *Z t. Finland*, § 95; grote kamer, 12 januari 2010, *S. en Marper t. Verenigd Koninkrijk*, § 103).

B.12.2. Een inmenging in het recht op eerbiediging van het privéleven door middel van een verwerking van persoonsgegevens, moet berusten op een redelijke verantwoording en dient evenredig te zijn met de door de wetgever nagestreefde doelstellingen. Wat de evenredigheid betreft, houdt het Europees Hof voor de Rechten van de Mens rekening met het al dan niet aanwezig zijn van waarborgen in de betrokken regeling ter voorkoming van misbruiken bij de verwerking van persoonsgegevens:

‘35. De bescherming van persoonsgegevens speelt een fundamentele rol voor de uitoefening van het recht op eerbiediging van het privé- en gezinsleven, dat is vastgelegd bij artikel 8 van het Verdrag. De interne wetgeving moet dus in gepaste waarborgen voorzien om elk gebruik van persoonsgegevens dat niet zou overeenstemmen met de in dat artikel bepaalde waarborgen, te verhinderen. Die noodzaak is des te groter wanneer het gaat om de bescherming van persoonsgegevens die automatisch worden verwerkt, in het bijzonder wanneer die gegevens worden gebruikt voor politieke doeleinden. Het interne recht moet meer bepaald ervoor zorgen dat die gegevens ter zake dienend en niet overmatig zijn uitgaande van de doeleinden waarvoor zij worden opgeslagen, en dat zij worden bewaard in een zodanige vorm dat de betrokkene hierdoor niet langer te identificeren is dan strikt noodzakelijk is voor het doel waarvoor de gegevens zijn opgeslagen. Het interne recht moet ook waarborgen bevatten om de opgeslagen persoonsgegevens op doeltreffende wijze te beschermen tegen oneigenlijk gebruik en misbruik (*S. en Marper t. Verenigd Koninkrijk*, voormeld, § 103, *Gardel t. Frankrijk*, voormeld, § 62, EHRM 2009, en *M.K. t. Frankrijk*, voormeld, § 35).

36. Pour apprécier le caractère proportionné de la durée de conservation des informations au regard du but poursuivi par leur mémorisation, la Cour tient compte de l'existence ou non d'un contrôle indépendant de la justification de leur maintien dans le système de traitement, exercé sur la base de critères précis tels que la gravité de l'infraction, les arrestations antérieures, la force des soupçons pesant sur la personne ou toute autre circonstance particulière (*S. et Marper c. Royaume-Uni*, précité, § 119, et *B.B. c. France*, précité, § 68).

37. Enfin, il appartient à la Cour d'être particulièrement attentive au risque de stigmatisation de personnes qui, à l'instar du requérant, n'ont été reconnues coupables d'aucune infraction et sont en droit de bénéficier de la présomption d'innocence. Si, de ce point de vue, la conservation de données privées n'équivaut pas à l'expression de soupçons, encore faut-il que les conditions de cette conservation ne leur donne pas l'impression de ne pas être considérés comme innocents (*S. et Marper*, précité, § 122, et *M.K.*, précité, § 36) (CEDH, 18 septembre 2014, *Brunet c. France*, §§ 35-37).

Pour juger du caractère proportionné de mesures relatives au traitement de données à caractère personnel dans des banques de données par les services de police, il convient dès lors de tenir compte notamment de la pertinence et du caractère excessif ou non des données traitées, de l'existence ou de l'absence de mesures qui limitent la durée de conservation des données, de l'existence ou de l'absence d'un système de contrôle indépendant permettant de vérifier si la conservation des données est encore requise, de la présence ou de l'absence de garanties visant à éviter la stigmatisation des personnes dont les données sont traitées et de la présence ou de l'absence de garanties visant à éviter l'usage abusif, par les services de police, des données à caractère personnel traitées (CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, § 59; grande chambre, 12 janvier 2010, *S. et Marper c. Royaume-Uni*, §§ 101-103, 119, 122 et 124; 18 avril 2013, *M.K. c. France*, §§ 37 et 42-44)³³.

Ainsi que le précise l'exposé des motifs, le dispositif en projet a pour objet de préciser, d'explicitier et de développer certains aspects actuellement prévus par la loi du 5 août 1992 'sur la fonction de police' ou par la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel' pour garantir la protection des données dans le cadre du fonctionnement de la banque de données commune T.E.R.

À propos du traitement des données à caractère personnel, il est posé, à l'article 6, § 1^{er}, le principe suivant:

"La banque de données commune T.E.R. nécessite le traitement de différentes catégories de données à caractère personnel relatives aux personnes, aux groupements, aux organisations et aux phénomènes qui sont adéquates, pertinentes

36. Om het evenredige karakter van de bewaringstermijn van de informatie te beoordelen in het licht van het doel dat met het opslaan van die informatie wordt nagestreefd, houdt het Hof rekening met het al dan niet voorhanden zijn van een onafhankelijke controle op de verantwoording voor het behoud ervan in het verwerkingssysteem, controle die wordt uitgeoefend op grond van precieze criteria zoals de ernst van het misdrijf, de vroegere arrestaties, de mate van verdenking die op de persoon weegt, of enige andere bijzondere omstandigheid (*S. en Marper t. Verenigd Koninkrijk*, voormeld, § 119, en *B.B. t. Frankrijk*, voormeld, § 68).

37. Ten slotte komt het Hof toe bijzondere aandacht te hebben voor het risico van stigmatisering van personen die, zoals de verzoeker, niet schuldig zijn bevonden aan enig misdrijf en het vermoeden van onschuld kunnen genieten. Ook al staat, uit dat oogpunt, het bewaren van privégegevens niet gelijk met het uiten van een verdenking, toch mogen de voorwaarden van die bewaring niet de indruk geven dat die personen niet als onschuldig worden beschouwd (*S. en Marper*, voormeld, § 122, en *M.K.*, voormeld, § 36) (EHRM, 18 september 2014, *Brunet t. Frankrijk*, §§ 35-37).

Bij de beoordeling van de evenredigheid van maatregelen met betrekking tot de verwerking van persoonsgegevens in databanken door de politiediensten, dient aldus rekening te worden gehouden met, onder meer, de pertinentie en het al dan niet buitensporige karakter van de gegevens die worden verwerkt, het al dan niet voorhanden zijn van maatregelen die de duur van de bewaring van de gegevens beperken, het al dan niet voorhanden zijn van een systeem van onafhankelijk toezicht dat toelaat na te gaan of de bewaring van de gegevens nog langer is vereist, het al dan niet voorhanden zijn van waarborgen ter voorkoming van stigmatisering van de personen van wie de gegevens worden verwerkt, en het al dan niet voorhanden zijn van waarborgen ter voorkoming van foutief gebruik door de politiediensten van de verwerkte persoonsgegevens (EHRM, grote kamer, 4 mei 2000, *Rotaru t. Roemenië*, § 59; grote kamer, 12 januari 2010, *S. en Marper t. Verenigd Koninkrijk*, §§ 101-103, 119, 122 en 124; 18 april 2013, *M.K. t. Frankrijk*, §§ 37 en 42-44)³³.

Zoals in de memorie van toelichting wordt uiteengezet, strekt het ontworpen dispositief tot precisering, explicitering en uitwerking van sommige aspecten die momenteel worden bepaald door de wet van 5 augustus 1992 'op het politieambt' of door de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens' om ervoor te zorgen dat de werkwijze van de gemeenschappelijke gegevensbank T.E.R. garanties inhoudt voor de gegevensbescherming.

In verband met de verwerking van persoonsgegevens wordt in artikel 6, § 1, als principe het volgende gesteld:

"De gemeenschappelijke gegevensbank T.E.R. vereist de verwerking van verschillende categorieën van persoonsgegevens met betrekking tot personen, groeperingen, organisaties en fenomenen die toereikend, ter zake dienend en niet overmatig

³³ C.C., 14 juillet 2016, n°108/2016, B.12.

³³ GwH 14 juli 2016, nr. 108/2016, B.12.

et non excessives au regard des missions visées à l'article 3, et des finalités visées à l'article 5, alinéa 2.

Les données à caractère personnel visées à l'alinéa 1^{er} présentent un lien direct avec la finalité du traitement”.

Il est rappelé que le traitement ne peut porter que sur des données à caractère personnel et informations relatives aux missions de prévention et de suivi du terrorisme et de l'extrémisme lorsqu'il peut mener au terrorisme par les services concernés dans le cadre exclusif de leurs compétences légales (article 3, alinéa 1^{er}, de l'avant-projet) et dans le respect strict des quatre finalités énumérées à l'article 5, alinéa 2, de l'avant-projet (1° la concertation coordonnée entre les services de base et les services partenaires; 2° la nécessité stratégique, tactique ou opérationnelle de traiter en commun des données à caractère personnel et des informations pour exercer les missions respectives des services de base et des services partenaires; 3° l'aide à la prise de décisions par les autorités administratives ou à la prise de décisions de police administrative ou judiciaire; 4° l'analyse, l'évaluation et le suivi, en ce compris la prise de mesures, des “entités” enregistrées dans la banque de données commune T.E.R. et l'analyse, l'évaluation et le suivi du phénomène du terrorisme et de l'extrémisme lorsqu'il peut mener au terrorisme sur base d'une évaluation de la menace).

Concernant la durée strictement nécessaire de conservation, il est prévu que les données à caractère personnel conservées dans la banque de données commune T.E.R. sont archivées dès que les finalités visées à l'article 5, alinéa 2, ne sont plus rencontrées et au maximum trente ans après le dernier traitement, à l'exception des données à caractère personnel relatives à des mineurs, qui sont conservées au maximum quinze ans après le dernier traitement (article 7, § 1^{er}, de l'avant-projet). Après le dernier traitement, le responsable opérationnel (à savoir l'Organe de la coordination pour l'analyse de la menace, qui, selon l'exposé des motifs, sera désigné en cette qualité en application de l'article 12 de l'avant-projet) examine tous les cinq ans (tous les trois ans pour les mineurs) si les données à caractère personnel présentent toujours un lien direct avec l'une des finalités de l'article 5, alinéa 2, et, si tel n'est pas le cas, les données sont archivées (article 7, § 1^{er}, alinéas 2 et 3, de l'avant-projet).

Pour éviter un usage abusif des données, il ressort des informations transmises par la déléguée du ministre qu'il sera prévu, en exécution de l'article 6, § 2, alinéa 5, de l'avant-projet, ce qui suit:

“Pour faciliter la gestion des accès, chaque service devra identifier les membres de son personnel autorisés à exercer les droits d'accès à la banque de données commune T.E.R. et devra transmettre une liste de ces personnes au gestionnaire qui gère les accès. Les membres du personnel doivent être titulaires d'une habilitation de sécurité de niveau ‘secret’ sauf pour les services de police afin de leur permettre d'évaluer correctement l'attitude à adopter à l'égard d'une personne dans les situations d'urgence” (voir, par ailleurs, le contenu des

zijn in verhouding tot de opdrachten bedoeld in artikel 3, en de doeleinden bedoeld in artikel 5, tweede lid.

De persoonsgegevens bedoeld in het eerste lid staan in rechtstreeks verband met het doeleinde van de verwerking.”

Er wordt aan herinnerd dat de verwerking enkel mogelijk is als ze betrekking heeft op persoonsgegevens en informatie betreffende opdrachten inzake de voorkoming en de opvolging van terrorisme en van extremisme ingeval dat tot terrorisme kan leiden, als ze wordt verricht door de betrokken diensten binnen het exclusieve kader van hun wettelijke bevoegdheden (artikel 3, eerste lid, van het voorontwerp), en met strikte inachtneming van de vier doeleinden die in artikel 5, tweede lid, van het voorontwerp worden opgesomd (1° het gecoördineerde overleg tussen de basisdiensten en de partnerdiensten; 2° de strategische, tactische of operationele noodzaak om gezamenlijk persoonsgegevens en informatie te verwerken voor het uitoefenen van de respectieve opdrachten van de basisdiensten en de partnerdiensten; 3° de hulp bij het nemen van beslissingen door de bestuurlijke overheden of bij het nemen van beslissingen van bestuurlijke of gerechtelijke politie; 4° de analyse, de evaluatie en de opvolging, daaronder begrepen het nemen van maatregelen, van de in de gemeenschappelijke gegevensbank T.E.R. geregistreerde “entiteiten” en de analyse, de evaluatie en de opvolging van het fenomeen van terrorisme en extremisme ingeval het tot terrorisme kan leiden, op grond van een dreigingsevaluatie).

Wat de strikt noodzakelijke bewaringstermijn betreft, wordt bepaald dat de in de gemeenschappelijke gegevensbank T.E.R. bewaarde persoonsgegevens worden gearchiveerd vanaf het ogenblik dat de doeleinden bedoeld in artikel 5, tweede lid, niet meer worden bereikt, en ten hoogste dertig jaar na de laatste verwerking, met uitzondering van de persoonsgegevens van minderjarigen, die tot maximaal vijftien jaar na de laatste verwerking worden bewaard (artikel 7, § 1, van het voorontwerp). Na de laatste verwerking onderzoekt de operationeel verantwoordelijke (namelijk het Coördinatieorgaan voor de dreigingsanalyse, dat volgens de memorie van toelichting met toepassing van artikel 12 van het voorontwerp in deze hoedanigheid zal worden aangewezen) om de vijf jaar (om de drie jaar voor minderjarigen) of de persoonsgegevens nog steeds een rechtstreeks verband vertonen met een van de doeleinden van artikel 5, tweede lid, en, als dat niet het geval is, worden de gegevens gearchiveerd (artikel 7, § 1, tweede en derde lid, van het voorontwerp).

Om onrechtmatig gebruik van de gegevens te voorkomen, zal, blijkens de inlichtingen die de gemachtigde van minister heeft verstrekt, in uitvoering van artikel 6, § 2, vijfde lid, van het voorontwerp het volgende worden bepaald:

“Pour faciliter la gestion des accès, chaque service devra identifier les membres de son personnel autorisés à exercer les droits d'accès à la banque de données commune T.E.R. et devra transmettre une liste de ces personnes au gestionnaire qui gère les accès. Les membres du personnel doivent être titulaires d'une habilitation de sécurité de niveau ‘secret’ sauf pour les services de police afin de leur permettre d'évaluer correctement l'attitude à adopter à l'égard d'une personne dans les situations d'urgence” (zie voorts de inhoud van

fichiers de journalisation décrit par l'article 8, § 1^{er}, alinéa 2, 2°, de l'avant-projet).

Enfin, les autorités de contrôle sont, en vertu de l'article 2, 15°, de l'avant-projet, l'Organe de contrôle de l'information policière visé à l'article 71 de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel' et le Comité permanent de contrôle des services de renseignements et de sécurité visé à l'article 1^{er} de la loi du 18 juillet 1991 'organique du contrôle des services de police et de renseignement et de l'Organe de coordination de la menace'.

Au stade préventif du contrôle exercé par la section de législation du Conseil d'État, il n'apparaît pas dans ce contexte que l'avant-projet ne respecterait pas le principe de proportionnalité inhérent à toute intrusion dans le droit au respect de la vie privée.

III. — Quant aux habilitations au Roi

1. L'avant-projet contient plusieurs habilitations au Roi.

Il est renvoyé aux observations générales n^{os} 2.4 à 2.7 pour ce qui concerne leur admissibilité au regard du principe de légalité déduit de l'article 22 de la Constitution.

2. Certaines habilitations appellent en outre, en tout état de cause, l'observation suivante.

La déléguée du ministre a admis que plusieurs d'entre elles s'avèrent inutiles ou font double emploi avec d'autres.

Tel est le cas des habilitations contenues dans les dispositions suivantes:

– l'article 8, § 1^{er}, alinéa 4:

“Le Roi peut, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, déterminer d'autres types de traitements pour lesquels les fichiers de journalisation sont établis”;

– l'article 10:

“Le Roi peut, par arrêté royal délibéré en Conseil des ministres et après avis des autorités de contrôle, déterminer des modalités complémentaires de gestion de la banque de données commune T.E.R.”;

– l'article 18, alinéa 2:

“Le Roi détermine, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, les modalités d'exercice du droit de création visé à l'alinéa premier”;

– l'article 28, § 4:

de logbestanden, beschreven in onder meer artikel 8, § 1, tweede lid, 2°, van het voorontwerp).

Tot slot zijn de toezichthoudende overheden, krachtens artikel 2, 15°, van het voorontwerp, het Controleorgaan op de politieke informatie, bedoeld in artikel 71 van de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens', en het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, bedoeld in artikel 1 van de wet van 18 juli 1991 'tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse'.

In het preventieve stadium van de controle die de afdeling Wetgeving van de Raad van State uitvoert, blijkt in dat verband niet dat het voorontwerp het evenredigheidsbeginsel, dat inherent is aan elke inmenging in het recht op eerbiediging van het privéleven, niet in acht zou nemen.

III. — Machtigingen verleend aan de Koning

1. Het voorontwerp verleent verscheidene machtigingen aan de Koning.

Voor wat betreft hun toelaatbaarheid in het licht van het legaliteitsbeginsel dat uit artikel 22 van de Grondwet voortvloeit, wordt verwezen naar de algemene opmerkingen 2.4 tot 2.7.

2. Voorts geven sommige machtigingen hoe dan ook aanleiding tot de volgende opmerking.

De gemachtigde van de minister heeft toegegeven dat verscheidene van die machtigingen overbodig blijken te zijn of andere machtigingen overlappen.

Dat is het geval met de machtigingen die in de volgende bepalingen vervat zijn:

– artikel 8, § 1, vierde lid:

“De Koning kan, bij een in Ministerraad overlegd besluit en na advies van de toezichthoudende overheden, andere types van verwerking bepalen waarvoor logbestanden moeten worden opgesteld”;

– artikel 10:

“De Koning kan, bij een in Ministerraad overlegd besluit en na advies van de toezichthoudende overheden, bijkomende nadere beheersregels van de gemeenschappelijke gegevensbank T.E.R. bepalen”;

– artikel 18, tweede lid:

“De Koning bepaalt, bij een in Ministerraad overlegd besluit en na advies van de toezichthoudende overheden, de nadere regels voor het creatierecht bedoeld in het eerste lid”;

– artikel 28, § 4:

“Le Roi peut déterminer les modalités de la communication visée aux § 2 et § 3”;

– l'article 29, § 2, 3°:

“En complément des dispositions de l'article 157 de la loi relative à la protection des données, le délégué à la protection des données est chargé:

[...]

3° de l'exécution des autres missions relatives à la protection des données et à la sécurisation qui sont déterminées par le Roi ou qui lui sont confiées par les ministres de l'Intérieur et de la Justice”;

– l'article 32, § 2, alinéa 2:

“Le Roi peut, par arrêté délibéré en Conseil des ministres, déterminer d'autres missions de la TFL”;

– l'article 54, alinéa 1^{er}:

“Le Roi peut remplacer les références existantes dans les lois aux dispositions de la loi sur la fonction de police par les références aux dispositions correspondantes de la présente loi”.

Ces habilitations au Roi seront omises.

En conséquence, elles ne sont pas examinées dans la suite du présent avis, en ce compris quant à leur compatibilité avec le principe de légalité.

OBSERVATIONS PARTICULIÈRES

Article 2

1. Le commentaire de l'article 2 ne contient pas d'explication sur la nécessité de considérer les services visés à l'article 2, 3°, i) et j) (respectivement “le service des cultes et de la laïcité du Service [p]ublic fédéral Justice” et “l'Administration générale de la Trésorerie du Service [p]ublic fédéral Finances”), comme étant des services partenaires.

Interrogée à ce propos, la déléguée du ministre a répondu ce qui suit:

“L'exposé des motifs sera précisé pour ces partenaires.

Pour le service des cultes, la motivation est la suivante: [I] e Service des Cultes et de la Laïcité du SPF Justice, service partenaire doit pouvoir bénéficier d'un droit d'interrogation dans la banque de données commune T.E.R. Le service des Cultes et de la Laïcité du SPF Justice est légalement compétent pour la reconnaissance des cultes et des organisations non confessionnelles. Il paie en outre les traitements des ministres des cultes et des délégués des communautés philosophiques

“De Koning kan de nadere regels van de in § 2 en § 3 bedoelde mededeling bepalen”;

– artikel 29, § 2, 3°:

“Aanvullend op de bepalingen van artikel 157 van de wet gegevensbescherming wordt de functionaris voor gegevensbescherming belast met de volgende opdrachten:

(...)

3° het uitvoeren van andere opdrachten inzake de bescherming en beveiliging van gegevens die bepaald worden door de Koning of die hem door de ministers van Binnenlandse Zaken en Justitie worden toevertrouwd”;

– artikel 32, § 2, tweede lid:

“De Koning kan, bij een in Ministerraad overlegd besluit, andere opdrachten van de LTF bepalen”;

– artikel 54, eerste lid:

“De Koning kan de bestaande verwijzingen in wetten naar bepalingen van de wet op het politieambt vervangen door verwijzingen naar de ermee overeenstemmende bepalingen van deze wet.”

Die aan de Koning verleende machtigingen moeten worden weggelaten.

Bijgevolg worden ze verderop in dit advies niet onderzocht, ook niet wat betreft hun verenigbaarheid met het legaliteitsbeginsel.

BIJZONDERE OPMERKINGEN

Artikel 2

1. In de bespreking van artikel 2 wordt niet uitgelegd waarom het nodig is de in artikel 2, 3°, i) en j), beoogde diensten (respectievelijk “de dienst Erediensten en Vrijzinnigheid van de Federale Overheidsdienst Justitie” en “de Algemene administratie van de Thesaurie van de Federale Overheidsdienst Financiën”) te beschouwen als partnerdiensten.

Op een vraag daarover heeft de gemachtigde van de minister het volgende geantwoord:

“L'exposé des motifs sera précisé pour ces partenaires.

Pour le service des cultes, la motivation est la suivante: [I] e Service des Cultes et de la Laïcité du SPF Justice, service partenaire doit pouvoir bénéficier d'un droit d'interrogation dans la banque de données commune T.E.R. Le service des Cultes et de la Laïcité du SPF Justice est légalement compétent pour la reconnaissance des cultes et des organisations non confessionnelles. Il paie en outre les traitements des ministres des cultes et des délégués des communautés philosophiques

non confessionnelles. Dans le cadre de ses compétences, il est nécessaire que ce service puisse interroger la banque de données commune T.E.R.

Pour la trésorerie, la motivation est la suivante: [I]'Administration générale de la Trésorerie, l'autorité compétente en matière de sanctions financières par le gel des fonds et des ressources économiques des personnes et entités qui commettent ou tentent de commettre des infractions terroristes, les facilitent ou y participent, aura un droit de lecture et d'écriture dans la banque de données commune T.E.R., en tant que service partenaire. La trésorerie est gestionnaire des sanctions financières et acquiert donc à cet effet la connaissance d'infractions et de données à caractère financier qui doivent être centralisées dans la banque de données commune pour assurer un échange de données intégré et optimal.

Dans la pratique, les avoirs de toutes les personnes qui ont rejoint un groupe terroriste en Syrie/Irak (FTF catégorie 1) ont été gelés. En outre, les avoirs d'un certain nombre d'autres entités ont déjà été gelés, notamment les avoirs de personnes condamnées pour des infractions terroristes. En outre, la Trésorerie est régulièrement contactée par des institutions financières lorsqu'elles entrent en contact avec des personnes dont les avoirs ont été gelés (ou pour lesquelles d'autres mesures financières ont été prises) par d'autres États (par exemple les États-Unis) dans un contexte de terrorisme, mais pas en Belgique. La Trésorerie doit procéder aux vérifications nécessaires et informer les institutions financières des conséquences éventuelles. L'un des éléments importants à cet égard est l'information consistant à savoir si la personne a été ou non reprise dans la banque de données commune T.E.R. La Trésorerie doit alors avoir la possibilité de vérifier quelles entités sont reprises en tant que telles dans la banque de données commune T.E.R.

Par ailleurs, l'Administration générale de la Trésorerie doit avoir la possibilité d'insérer elle-même les décisions qu'elle prend ainsi que de nombreuses informations pertinentes recueillies dans le cadre de sa compétence en matière de sanctions financières comme décrit dans l'arrêté royal du 28 décembre 2006 relatif aux mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le financement du terrorisme et la loi du 13 mai 2003 relative à la mise en œuvre des mesures restrictives adoptées par le Conseil de l'Union européenne à l'encontre d'États, de certaines personnes et entités. Sont visés ici: des montants financiers gelés, d'éventuels mouvements sur des comptes bancaires ou encore des assurances de tout type faisant l'objet d'une mesure de gel dans cette banque de données commune. Il est évident que ceci porte uniquement sur les informations relatives aux entités ayant déjà été reprises dans la Banque de données commune selon la procédure appropriée.

L'exposé des motifs et le commentaire seront complétés en conséquence.

2. L'article 2, 4°, définit l'"entité" notamment comme étant "toute personne physique majeure ou mineure de plus de douze ans".

non confessionnelles. Dans le cadre de ses compétences, il est nécessaire que ce service puisse interroger la banque de données commune T.E.R.

Pour la trésorerie, la motivation est la suivante: [I]'Administration générale de la Trésorerie, l'autorité compétente en matière de sanctions financières par le gel des fonds et des ressources économiques des personnes et entités qui commettent ou tentent de commettre des infractions terroristes, les facilitent ou y participent, aura un droit de lecture et d'écriture dans la banque de données commune T.E.R., en tant que service partenaire. La trésorerie est gestionnaire des sanctions financières et acquiert donc à cet effet la connaissance d'infractions et de données à caractère financier qui doivent être centralisées dans la banque de données commune pour assurer un échange de données intégré et optimal.

Dans la pratique, les avoirs de toutes les personnes qui ont rejoint un groupe terroriste en Syrie/Irak (FTF catégorie 1) ont été gelés. En outre, les avoirs d'un certain nombre d'autres entités ont déjà été gelés, notamment les avoirs de personnes condamnées pour des infractions terroristes. En outre, la Trésorerie est régulièrement contactée par des institutions financières lorsqu'elles entrent en contact avec des personnes dont les avoirs ont été gelés (ou pour lesquelles d'autres mesures financières ont été prises) par d'autres États (par exemple les États-Unis) dans un contexte de terrorisme, mais pas en Belgique. La Trésorerie doit procéder aux vérifications nécessaires et informer les institutions financières des conséquences éventuelles. L'un des éléments importants à cet égard est l'information consistant à savoir si la personne a été ou non reprise dans la banque de données commune T.E.R. La Trésorerie doit alors avoir la possibilité de vérifier quelles entités sont reprises en tant que telles dans la banque de données commune T.E.R.

Par ailleurs, l'Administration générale de la Trésorerie doit avoir la possibilité d'insérer elle-même les décisions qu'elle prend ainsi que de nombreuses informations pertinentes recueillies dans le cadre de sa compétence en matière de sanctions financières comme décrit dans l'arrêté royal du 28 décembre 2006 relatif aux mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le financement du terrorisme et la loi du 13 mai 2003 relative à la mise en œuvre des mesures restrictives adoptées par le Conseil de l'Union européenne à l'encontre d'États, de certaines personnes et entités. Sont visés ici: des montants financiers gelés, d'éventuels mouvements sur des comptes bancaires ou encore des assurances de tout type faisant l'objet d'une mesure de gel dans cette banque de données commune. Il est évident que ceci porte uniquement sur les informations relatives aux entités ayant déjà été reprises dans la Banque de données commune selon la procédure appropriée."

De memorie van toelichting en de bespreking moeten dienovereenkomstig worden aangevuld.

2. In artikel 2, 4°, wordt "entiteit" gedefinieerd als onder meer "elke meerderjarige natuurlijke persoon of minderjarige natuurlijke persoon ouder dan twaalf jaar".

Aux termes du commentaire de l'article, les personnes ainsi visées sont les mineurs de douze ans et plus³⁴ et non "de plus de douze ans"; le dispositif sera revu en ce sens. C'est dans cette lecture que l'observation qui suit est formulée.

L'avant-projet instaure ainsi une différence de traitement entre les mineurs, avec pour conséquence qu'ils ne seront enregistrés dans la banque de données commune T.E.R. qu'à la double condition d'avoir atteint l'âge de douze ans³⁵ et que les autres conditions liées à l'enregistrement d'une entité soient réunies³⁶.

Pareil dispositif doit être mis en rapport avec les considérations suivantes émises par la Cour constitutionnelle:

"B.148.1. [...] [U]n traitement de données à caractère personnel dans des banques de données policières ne peut être considéré ni comme une incrimination, ni comme une peine au sens des articles 12 et 14 de la Constitution, étant donné qu'il constitue seulement une mesure à caractère préventif ou une mesure d'investigation.

En permettant le traitement des données à caractère personnel de mineurs dans les banques de données policières, la loi attaquée n'instaure donc pas une incrimination ou une peine qui dérogerait aux dispositions de la loi relative à la protection de la jeunesse, laquelle reste intégralement applicable.

[...]

B.149. Tant l'article 22*bis*, alinéa 4, de la Constitution que l'article 3, paragraphe 1, de la Convention relative aux droits de l'enfant imposent aux autorités de prendre en compte, de manière primordiale, l'intérêt de l'enfant dans les procédures le concernant. L'article 22*bis*, alinéa 5, de la Constitution donne par ailleurs au législateur la mission de garantir que l'intérêt de l'enfant soit pris en considération de manière primordiale.

Ces dispositions n'empêchent pas en elles-mêmes le législateur de prévoir que des données à caractère personnel de mineurs peuvent être traitées par les services de police, afin de permettre à ces services de remplir leurs missions légales. Ces missions, qui portent notamment sur le maintien de l'ordre public, la protection des personnes et des biens et la prévention et la recherche d'infractions, ne sont pas, par nature, exclusivement liées aux actes et comportements des personnes majeures.

Cependant, lorsqu'il établit les circonstances dans lesquelles des données à caractère personnel peuvent être traitées par les services de police, le législateur doit tenir compte de

Luidens de bespreking van het artikel zijn de aldus beoogde personen minderjarigen van twaalf jaar of ouder³⁴ en niet "ouder dan twaalf jaar"; het dispositief moet in die zin worden herzien. Het is in het kader van die acceptie dat de hiernavolgende opmerking wordt geformuleerd.

Het voorontwerp voert aldus een verschil in behandeling in tussen minderjarigen onderling, met als gevolg dat dezen pas in de gemeenschappelijke gegevensbank T.E.R. zullen worden geregistreerd als ze de leeftijd van twaalf jaar hebben bereikt³⁵ én als daarbovenop de andere voorwaarden met betrekking tot de registratie van een entiteit worden vervuld.³⁶

In verband met een dergelijk dispositief moet worden gewezen op de hiernavolgende overwegingen van het Grondwettelijk Hof:

"B.148.1. (...) [E]en verwerking van persoonsgegevens in politionele databanken [kan] niet worden beschouwd als een strafbaarstelling, noch als een strafsancie in de zin van de artikelen 12 en 14 van de Grondwet, aangezien zij slechts een maatregel van preventieve of onderzoekende aard is.

Door een verwerking van de persoonsgegevens van minderjarigen in de politionele databanken toe te laten, voert de bestreden wet aldus geen strafbaarstelling of strafsancie in die zou afwijken van de bepalingen van de Jeugdbeschermingswet, die onverkort van toepassing blijft.

(...)

B.149. Zowel artikel 22*bis*, vierde lid, van de Grondwet als artikel 3, lid 1, van het Verdrag inzake de rechten van het kind verplichten de overheid om in de eerste plaats het belang van het kind in aanmerking te nemen bij elke beslissing die het kind aangaat. Artikel 22*bis*, vijfde lid, van de Grondwet geeft de wetgever overigens de opdracht te waarborgen dat het belang van het kind de eerste overweging is.

Die bepalingen verhinderen op zich de wetgever niet te bepalen dat persoonsgegevens van minderjarigen door de politiediensten kunnen worden verwerkt teneinde die diensten toe te laten hun wettelijke opdrachten te vervullen. Die opdrachten, die onder meer betrekking hebben op de handhaving van de openbare orde, de bescherming van personen en goederen en het voorkomen en het opsporen van misdrijven, houden, uit hun aard, niet uitsluitend verband met handelingen en gedragingen van meerderjarigen.

Niettemin dient de wetgever, bij het bepalen van de omstandigheden waarin persoonsgegevens door de politiediensten kunnen worden verwerkt, rekening te houden met de bijzondere

³⁴ Voir ci-dessous.

³⁵ Sous réserve de l'article 6, § 2, alinéa 1^{er}, 1°, 1), b).

³⁶ Ce n'est qu'en cas d'indices qu'une personne représente une menace pour la sécurité nationale que celle-ci y figurera (exposé des motifs, p. 14).

³⁴ Zie hieronder.

³⁵ Onder voorbehoud van artikel 6, § 2, eerste lid, 1°, 1), b).

³⁶ Het is pas als er aanwijzingen zijn dat een persoon een gevaar vormt voor de nationale veiligheid, dat deze persoon in de gegevensbank wordt opgenomen (memorie van toelichting, 14).

la situation particulière des mineurs, notamment en ce qui concerne leur personnalité et leur degré de maturité”³⁷.

À propos du choix de l'âge à partir duquel une personne physique peut être enregistrée dans la banque de données commune T.E.R., le commentaire de l'article 2 expose ce qui suit:

“Ce projet de loi est aussi plus précis à propos des critères d'enregistrement dans la banque de données T.E.R. liés à l'âge d'une personne physique: les personnes physiques majeures et mineures à partir de douze ans peuvent être enregistrées dans la banque de données commune T.E.R. si elles correspondent aux critères d'enregistrement. Les mineurs de moins de 12 ans ne sont donc pas enregistrés comme entité dans la banque de données commune T.E.R. Pour les mineurs à partir de 12 ans jusqu'à 18 ans inclus, des mesures de protection additionnelles sont en outre prévues. Ainsi, le délai de conservation maximum dans la banque de données commune T.E.R. après le dernier traitement n'est pas de 30 ans mais de 15 ans et le responsable opérationnel est tenu d'évaluer la nécessité d'archiver les données le concernant tous les 3 ans minimum et pas tous les 5 ans. Enfin, lors de l'évaluation préalable à la communication de données via une carte d'information, le statut de minorité doit être pris en compte pour évaluer la nécessité de réaliser cette communication.

Le seuil de douze ans a été choisi car il s'agit d'un âge pivot repris dans diverses législations.

En effet, il s'agit de l'âge à partir duquel des mesures peuvent être prises à l'égard de mineurs suspectés d'avoir commis un fait qualifié infraction. Avant cet âge, on privilégie le renvoi vers l'aide aux mineurs en danger et on ne peut en tout cas pas placer l'enfant sur la base du fait qualifié infraction (art. 37, § 2, de la loi du 8 avril 1965 relative à la protection de la jeunesse, à la prise en charge des mineurs ayant commis un fait qualifié infraction et à la réparation du dommage causé par ce fait).

Par ailleurs, 12 ans est l'âge à partir duquel un enfant peut être associé dans diverses procédures le concernant. Par exemples, il doit donner son consentement à son adoption (art. 348-1 du Code civil), il doit être cité à comparaître devant le tribunal de la jeunesse en cas de procédure de mineur en danger ou de mineur poursuivi du chef d'un fait qualifié infraction (art. 46 de la loi du 8 avril 1965 relative à la protection de la jeunesse, à la prise en charge des mineurs ayant commis un fait qualifié infraction et à la réparation du dommage causé par ce fait), ou encore il doit être informé de son droit d'être entendu par le tribunal de la famille dans les procédures relatives à l'autorité parentale (art. 1004/1 du Code judiciaire).

³⁷ C.C., 14 juillet 2016, n° 108/2016, B.148.1 et B.149. Voir également C.C., 23 avril 2015, n° 44/2015, B.51.3.

situation van de minderjarigen, onder meer op het vlak van hun persoonlijkheid en hun maturiteitsgraad.”³⁷

Over de keuze van de leeftijd vanaf wanneer een natuurlijke persoon kan worden geregistreerd in de gemeenschappelijke gegevensbank T.E.R. staat in de bespreking van artikel 2 het volgende:

“Dit wetsontwerp schept tevens meer duidelijkheid rond de criteria van de opname in de gegevensbank T.E.R. met betrekking tot de leeftijd van een natuurlijke persoon: meerderjarige natuurlijke personen en minderjarige natuurlijke personen vanaf twaalf jaar kunnen in de gemeenschappelijke gegevensbank T.E.R. worden opgenomen als ze voldoen aan de opnamecriteria. Minderjarigen jonger dan twaalf jaar worden dus niet als entiteit in de gemeenschappelijke gegevensbank T.E.R. opgenomen. Voor minderjarigen van twaalf tot en met achttien jaar wordt er bovendien in extra beschermingsmaatregelen voorzien. Zo bedraagt de maximale bewaringstermijn in de gemeenschappelijke gegevensbank T.E.R. na de laatste verwerking niet dertig maar vijftien jaar en moet de operationeel verantwoordelijke de noodzakelijkheid om de gegevens te archiveren die op hem betrekking hebben, minimaal om de drie jaar en niet om de vijf jaar evalueren. Tot slot is het zo dat bij de evaluatie vóór de mededeling van gegevens via een informatiekaart rekening moet worden gehouden met het statuut van minderjarige om te beoordelen of het noodzakelijk is om die mededeling te doen.

Er werd geopteerd voor de ondergrens van twaalf jaar omdat dit een spilleeftijd die in verschillende wetgevingen wordt gehanteerd.

Vanaf die leeftijd kunnen immers maatregelen worden genomen ten aanzien van minderjarigen die verdacht worden van het plegen van een als misdrijf omschreven feit. Vóór die leeftijd wordt de voorkeur gegeven aan doorverwijzing naar hulpverlening aan minderjarigen in gevaar, en kan men het kind alleszins niet plaatsen op grond van het als misdrijf omschreven feit (art. 37, § 2, van de wet van 8 april 1965 betreffende de jeugdbescherming, het ten laste nemen van minderjarigen die een als misdrijf omschreven feit hebben gepleegd en het herstel van de door dit feit veroorzaakte schade).

Overigens geldt twaalf jaar als de leeftijd vanaf wanneer een kind kan betrokken worden bij diverse procedures die het aanbelangen. Zo moet het kind bijvoorbeeld toestemmen in zijn adoptie (art. 348-1 van het Burgerlijk Wetboek), het moet gedagvaard worden om te verschijnen voor de jeugdrechtsbank ingeval van procedure van minderjarige in gevaar of van minderjarige die wordt vervolgd wegens een als misdrijf omschreven feit (art. 46 van de wet van 8 april 1965 betreffende de jeugdbescherming, het ten laste nemen van minderjarigen die een als misdrijf omschreven feit hebben gepleegd en het herstel van de door dit feit veroorzaakte schade), en ook moet het kind ingelicht worden over zijn recht om gehoord te worden door de familierechtbank in de procedures aangaande het ouderlijk gezag (art. 1004/1 van het Gerechtelijk Wetboek).

³⁷ GwH 14 juli 2016, nr. 108/2016, B.148.1 en B.149. Zie eveneens GwH 23 april 2015, nr. 44/2015, B.51.3.

Au niveau international, le Comité des droits de l'enfant (chargé de surveiller l'application par les États de la Convention internationale des droits de l'enfant) a été très clair dans ses observations n° 10 (2017) relatives aux droits de l'enfant dans le système de justice pour mineurs.

Il précise ce qui suit (n° 32, page 54): '[l']article 4 des Règles de Beijing prescrit, dans les systèmes juridiques qui reconnaissent la notion de seuil de responsabilité pénale, de ne pas fixer ce seuil trop bas eu égard aux problèmes de maturité affective, psychologique et intellectuelle. Conformément à cette règle, le Comité a recommandé à des États parties de ne pas fixer à un niveau trop bas l'âge minimum de la responsabilité pénale ou bien de relever cet âge minimum, là où il est trop faible, pour le porter à un niveau acceptable sur le plan international. Il ressort de ces recommandations que le Comité considère comme inacceptable sur le plan international de fixer l'âge minimum de la responsabilité pénale en dessous de 12 ans. Des États parties sont encouragés à relever l'âge trop bas de la responsabilité pénale pour le porter à 12 ans, âge qui constitue un minimum absolu, et à continuer de le relever progressivement''.

La différence de traitement entre les mineurs selon qu'ils ont atteint ou non l'âge de douze ans semble raisonnablement justifiée en l'espèce au regard de la jurisprudence de la Cour constitutionnelle étant donné que le législateur peut en principe, pour fixer l'âge à partir duquel des données à caractère personnel peuvent être traitées dans un instrument tel que la banque de données commune T.E.R., s'inspirer de l'âge de douze ans qui est fixé dans les lois précitées³⁸.

Article 6

1. Au paragraphe 2, 1°, 1), a), ii., parmi les catégories de données pouvant être traitées, figure, "s'il échet, le numéro d'identification du registre national des personnes physiques".

La question se pose de savoir s'il n'y a pas lieu de prévoir également une identification liée à d'autres registres comme par exemple le registre des étrangers.

Interrogée à ce sujet, la déléguée du ministre a répondu que le numéro du registre des étrangers est une donnée qui permet aussi d'avoir une identification unique et qu'elle sera ajoutée à la liste.

L'article 6 sera complété en conséquence. Il en va de même pour le commentaire, qui doit contenir une justification quant à l'ajout de cette donnée supplémentaire.

2. L'article 6, § 2, alinéa 1^{er}, 1°, 1), c), énumère les données relatives aux catégories particulières de données à caractère personnel, dont les données concernant la santé (v.). Pour celles-ci, l'article 6, § 2, alinéa 2, prévoit dans quelles

Op internationaal niveau is het Comité voor de rechten van het kind (dat belast is met het toezicht op de toepassing van het Internationaal Verdrag inzake de Rechten van het Kind vanwege de Staten) zeer stellig geweest in zijn opmerkingen nr.10 (2017) betreffende de rechten van het kind binnen het rechtssysteem voor minderjarigen.

Het preciseert het volgende (nr. 32, bladzijde 54): 'Rule 4 of the Beijing Rules recommends that the beginning of MACR [minimum age of criminal responsibility] shall not be fixed at too low an age level, bearing in mind the facts of emotional, mental and intellectual maturity. In line with this rule the Committee has recommended States parties not to set a MACR at a too low level and to increase the existing low MACR to an internationally acceptable level. From these recommendations, it can be concluded that a minimum age of criminal responsibility below the age of 12 years is considered by the Committee not to be internationally acceptable. States parties are encouraged to increase their lower MACR to the age of 12 years as the absolute minimum age and to continue to increase it to a higher age level'.

Het verschil in behandeling tussen de minderjarigen onderling naargelang ze al dan niet de leeftijd van twaalf jaar hebben bereikt, lijkt *in casu* ten aanzien van de rechtspraak van het Grondwettelijk Hof redelijkerwijze verantwoord, aangezien de wetgever bij het vaststellen van de minimumleeftijd van personen wier persoonsgegevens mogen worden verwerkt in een instrument zoals de gemeenschappelijke gegevensbank T.E.R., zich in principe kan laten leiden door de leeftijd van twaalf jaar die in de voornoemde wetten wordt vastgesteld.³⁸

Artikel 6

1. Paragraaf 2, 1°, 1), a), ii., vermeldt als een van de categorieën van gegevens die mogen worden verwerkt, "indien van toepassing, het identificatienummer van het Rijksregister van de natuurlijke personen".

De vraag rijst of niet eveneens dient te worden voorzien in een identificatie die gekoppeld is aan andere registers, zoals bijvoorbeeld het vreemdelingenregister.

Op een vraag daarover heeft de gemachtigde van de minister geantwoord dat ook het nummer van het vreemdelingenregister een unieke identificatie mogelijk maakt en dat die identificatie aan de lijst moet worden toegevoegd.

Artikel 6 moet dienovereenkomstig worden aangevuld. Hetzelfde geldt voor de bespreking, waarin de toevoeging van dat extra gegeven moet worden verantwoord.

2. In artikel 6, § 2, eerste lid, 1°, 1), c), worden de gegevens opgesomd betreffende de bijzondere categorieën van persoonsgegevens, waaronder de gegevens over de gezondheid (v.). Wat die laatste gegevens betreft, bepaalt artikel 6, § 2,

³⁸ C.C., 14 juillet 2016, n° 108/2016, B.145 à B.156.

³⁸ GwH 14 juli 2016, nr. 108/2016, B.145 tot B.156.

limites ces données dites “sensibles” peuvent être récoltées et l’article 6, § 2, alinéa 3, énonce l’hypothèse dans laquelle elles peuvent être communiquées.

Ces données figurent parmi celles visées par l’article 9, paragraphes 1 et 2, du RGPD et par l’article 10 de la directive (UE) 2016/680 précitée³⁹.

Aux termes de l’article 10 de cette directive,

“[...] le traitement des données génétiques, des données biométriques aux fins d’identifier une personne physique de manière unique, des données concernant la santé [...] est autorisé uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement:

a) lorsqu’ils sont autorisés par le droit de l’Union ou le droit d’un État membre;

b) pour protéger les intérêts vitaux de la personne concernée ou d’une autre personne physique; ou

c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée⁴⁰.

Dans le RGPD, c’est l’article 9 qui règle le même objet en visant en son paragraphe 1 les mêmes traitements que ceux mentionnés à l’article 10 de la directive (UE) 2016/680 pour les interdire avant d’énoncer en son paragraphe 2 une série de cas de figure dans lesquels cette interdiction ne s’applique pas, notamment lorsque:

“i) le traitement est nécessaire pour des motifs d’intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l’Union ou du droit de l’État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel”.

³⁹ Sur le champ d’application du RGPD et de la directive (UE) 2016/680 précitée, il est renvoyé à l’observation générale n° II, B, 2.6.

⁴⁰ Voir aussi l’article 34, § 1^{er}, de la loi précitée du 30 juillet 2018, qui transpose l’article 10 de la directive. L’article 34 de la loi comprend également un paragraphe 2, rédigé comme suit: “§ 2. Les garanties nécessaires visées au paragraphe 1^{er} prévoient au moins que l’autorité compétente ou le responsable de traitement établisse une liste des catégories de personnes, ayant accès aux données à caractère personnel avec une description de leur fonction par rapport au traitement des données visées. Cette liste est tenue à la disposition de l’autorité de contrôle compétente.

L’autorité compétente veille à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées”.

tweede lid, binnen welke grenzen die zogeheten “gevoelige” gegevens mogen worden verzameld en bepaalt artikel 6, § 2, derde lid, in welk geval ze mogen worden meegedeeld.

Die gegevens maken deel uit van de gegevens die worden bedoeld in artikel 9, lid 1 en 2, van de AVG en in artikel 10 van de voornoemde richtlijn (EU) 2016/680.³⁹

Artikel 10 van die richtlijn luidt:

“(…) verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, gegevens over gezondheid (...) [is] slechts toegelaten wanneer de verwerking strikt noodzakelijk is, geschiedt met inachtneming van passende waarborgen voor de rechten en vrijheden van de betrokkene, en:

a) bij het Unierecht of het lidstatelijke recht is toegestaan;

b) noodzakelijk is om vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen; of

c) die verwerking betrekking heeft op gegevens die kennelijk door de betrokkene zelf openbaar zijn gemaakt.⁴⁰

In de AVG wordt datzelfde onderwerp geregeld bij artikel 9: in lid 1 vermeldt – en verbiedt – het dezelfde verwerkingen als die welke in artikel 10 van richtlijn (EU) 2016/680 worden opgegeven en in lid 2 somt het vervolgens een reeks gevallen op waarin dat verbod niet van toepassing is, onder meer wanneer:

“i) de verwerking (...) noodzakelijk [is] om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim.”

³⁹ Wat het toepassingsgebied van de AVG en van de voornoemde richtlijn (EU) 2016/680 betreft, wordt verwezen naar algemene opmerking II, B, 2.6.

⁴⁰ Zie ook artikel 34, § 1, van de voornoemde wet van 30 juli 2018, waarbij artikel 10 van de richtlijn wordt omgezet. Artikel 34 van de wet bevat eveneens een paragraaf 2, die als volgt luidt: “§ 2. De passende waarborgen zoals bedoeld in paragraaf 1 voorzien ten minste in dat de bevoegde overheid of de verwerkingsverantwoordelijke een lijst van de categorieën van personen die toegang hebben tot de persoonsgegevens opstelt, met een beschrijving van hun hoedanigheid ten opzichte van de verwerking van de beoogde gegevens. Deze lijst wordt ter beschikking gehouden van de bevoegde toezichthoudende autoriteit. De bevoegde overheid waakt erover dat de aangewezen personen door een wettelijke of statutaire verplichting, of door een evenwaardige contractuele bepaling ertoe gehouden zijn het vertrouwelijke karakter van de betrokken gegevens in acht te nemen.”

Le commentaire de l'article 6 de l'avant-projet explique ce qui suit:

“Le traitement de toutes les catégories particulières de données à caractère personnel précitées est assorti des garanties appropriées exigées par la loi relative à la protection des données. En effet, les données contenues dans la banque de données commune T.E.R. sont accessibles sur base de différents droits d'accès que le Roi va donner aux services énumérés dans la loi sur la base du principe du besoin d'en connaître pour l'exercice de leurs missions visées à l'article 3 et conformément aux finalités de l'article 5, alinéa 2. En outre, chaque service devra identifier les membres de son personnel autorisés à exercer les droits d'accès à la banque de données commune T.E.R. et devra transmettre une liste de ces personnes au gestionnaire qui gère les accès. Cette liste pourra, le cas échéant, être mise à la disposition du délégué à la protection des données et au responsable opérationnel dans le cadre de leurs missions respectives. Il est également précisé que les membres du personnel doivent être titulaires d'une habilitation de sécurité de niveau 'secret', pour accéder à la banque de données commune T.E.R.”

Pour les données dites “sensibles”, il y aura lieu de tenir compte, lors de la mise en œuvre de l'habilitation au Roi contenue dans l'article 6, § 2, alinéa 5, consistant à déterminer par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, les mesures nécessaires en vue d'assurer la gestion et la sécurité des données à caractère personnel et des informations traitées dans la banque de données communes T.E.R., des obligations imposées par l'article 10 de la directive 2016/680 et par l'article 9 du RGPD, spécialement le paragraphe 2, i), de cette dernière disposition. Cela implique, pour les traitements tombant dans le champ d'application de la directive, de prévoir des “garanties appropriées pour les droits et libertés de la personne concernée” et, pour ceux relevant du RGPD, de “prévoir[r] des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel”, compte tenu également de l'article 34, § 2, de la loi précitée du 30 juillet 2018.

Article 13

1. L'article 13, § 2, prévoit que le responsable opérationnel procède soit à une information (alinéas 1^{er} et 2), soit à une notification (alinéa 3) à des personnes ou à des organismes mentionnés quant à l'existence de “brèches de sécurité” de la banque de données commune T.E.R. Par ailleurs l'article 13, § 3, décrit le contenu de la notification “visée au paragraphe 2, alinéas 2 et 3”.

Or, l'alinéa 2 du paragraphe 2 utilise la notion d’“information” et non celle de “notification” et l'alinéa 1^{er} du paragraphe 2 ne serait donc pas concerné.

In de bespreking van artikel 6 van het voorontwerp staat het volgende:

“Voor de verwerking van alle bovengenoemde bijzondere categorieën van persoonsgegevens gelden de passende, bij de gegevensbeschermingswet opgelegde waarborgen. De gegevens in de gemeenschappelijke gegevensbank T.E.R. zijn namelijk toegankelijk op basis van verschillende toegangsrechten die de Koning de in de wet opgesomde diensten zal verlenen op basis van het principe van de behoefte om te kennen in het kader van de uitoefening van hun opdrachten bedoeld in artikel 3 en overeenkomstig de doeleinden van artikel 5, tweede lid. Voorts zal elke dienst moeten identificeren welke van zijn personeelsleden gemachtigd zijn om de toegangsrechten tot de gemeenschappelijke gegevensbank T.E.R. uit te oefenen en een lijst van die personen moeten bezorgen aan de beheerder van de toegangen. Die lijst kan, in voorkomend geval, ter beschikking worden gesteld van de functionaris voor gegevensbescherming en van de operationeel verantwoordelijke in het kader van hun respectieve opdrachten. Er wordt ook gepreciseerd dat de personeelsleden houder moeten zijn van een veiligheidsmachtiging van het niveau ‘geheim’ om toegang te kunnen krijgen tot de gemeenschappelijke gegevensbank T.E.R.”

Bij de tenuitvoerlegging van de machtiging die artikel 6, § 2, vijfde lid, aan de Koning verleent om, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van de toezichthoudende overheden, de maatregelen te bepalen die nodig zijn met het oog op het beheer en de veiligheid van de persoonsgegevens en de informatie die worden verwerkt in de gemeenschappelijk gegevensbank T.E.R., zal, wat de zogeheten “gevoelige” gegevens betreft, rekening dienen te worden gehouden met de verplichtingen opgelegd bij artikel 10 van richtlijn 2016/680 en bij artikel 9 van de AVG, in het bijzonder lid 2, i), van die laatste bepaling. Dat brengt met zich mee dat, voor de verwerkingen die in het toepassingsgebied van de richtlijn vallen, wordt voorzien in “passende waarborgen voor de rechten en vrijheden van de betrokkene” en dat, voor de verwerkingen die onder de AVG vallen, wordt voorzien in “passende en specifieke maatregelen (...) ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim”, eveneens rekening houdend met artikel 34, § 2, van de voornoemde wet van 30 juli 2018.

Artikel 13

1. Artikel 13, § 2, bepaalt dat de operationeel verantwoordelijke hetzij de vermelde personen of organismen in kennis stelt van de zich voordoende “inbreuken op de beveiliging” van de gemeenschappelijke gegevensbank T.E.R. (eerste en tweede lid), hetzij die inbreuken aan die personen of organismen meldt (derde lid). In artikel 13, § 3, wordt voorts de inhoud beschreven van “de in paragraaf 2, tweede en derde lid bedoelde melding”.

In het tweede lid van paragraaf 2 wordt echter de uitdrukking “in kennis stellen” gebruikt, en is er geen sprake van het begrip “melding”. Ook zou de “melding” waarnaar artikel 13, § 3, verwijst, dus niet slaan op het eerste lid van paragraaf 2.

Interrogée sur ce point, la déléguée du ministre a proposé d'harmoniser les paragraphes 2 et 3 pour viser uniquement la notification.

L'article 13 sera revu en conséquence.

2. Au paragraphe 2, alinéa 3, dès lors qu'il est prévu qu'en cas de brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable opérationnel est tenu de la notifier aux autorités de contrôle dans les meilleurs délais, il est inutile de préciser que cette notification doit être faite "si possible 72 heures après" que le responsable opérationnel en ait eu connaissance. Ainsi rédigé, ce membre de phrase pourrait en outre être interprété comme impliquant que la notification doit intervenir au plus tôt dans ce délai, ce qui manquerait de pertinence.

Les mots "et si possible, 72 heures après en avoir pris connaissance" seront omis.

Article 16

L'article 16 de l'avant-projet octroie aux autorités de contrôle exclusivement un droit de lecture dans la banque de données commune active ainsi que dans les archives.

Or, il est expliqué à plusieurs reprises dans l'exposé des motifs que le droit de lecture est toujours lié au droit d'écriture⁴¹.

Comme en a convenu la déléguée du ministre, tel n'est pas le cas dans le cadre de l'article 16, qui constitue donc une exception puisque le binôme "droit de lecture/droit d'écriture" ne vaut pas pour les organes de contrôles vu leur fonction de contrôle, qui ne nécessite pas un droit d'écriture mais uniquement un droit de lecture.

L'exposé des motifs et le commentaire seront clarifiés en conséquence.

Article 19

1. En introduisant le membre de phrase "qui bénéficient d'un droit de lecture et d'un droit d'écriture" par une virgule, l'alinéa 1^{er} doit être lu comme signifiant que non seulement les services de base mais également les services partenaires disposent nécessairement de ces droits.

Or, aux termes de l'article 17, ces services ne deviennent titulaires de ces droits que si le Roi le leur accorde.

⁴¹ Voir par exemple le commentaire introductif de la section 5 du chapitre 2 ("le droit de lecture va de pair avec le droit/l'obligation d'écriture") et le commentaire de l'article 17 ("les droits de lecture et d'écriture sont indissociables").

Naar aanleiding van een vraag daarover heeft de gemachtigde van de minister voorgesteld om de paragrafen 2 en 3 met elkaar in overeenstemming te brengen door alleen gebruik te maken van het begrip "melding".

Artikel 13 moet dienovereenkomstig worden herzien.

2. Aangezien in paragraaf 2, derde lid, wordt bepaald dat in geval van een inbreuk op de beveiliging die aanleiding kan vormen tot een hoog risico voor de rechten en vrijheden van natuurlijke personen, de operationeel verantwoordelijke deze inbreuk zo snel mogelijk moet melden aan de toezichthoudende overheden, heeft het geen zin om nog eens te specificeren dat dat moet gebeuren "indien mogelijk (...) 72 uur nadat" de operationeel verantwoordelijke er kennis van heeft genomen. Zoals dat zinsstuk gesteld is, zou men het bovendien zo kunnen interpreteren dat die melding ten vroegste 72 uur na de kennisneming hoort te worden gedaan, wat geen steek zou houden.

De woorden "en indien mogelijk, 72 uur nadat hij er kennis van heeft genomen" moeten worden weggelaten.

Artikel 16

Bij artikel 16 van het voorontwerp wordt aan de toezichthoudende overheden uitsluitend een leesrecht met betrekking tot de actieve gemeenschappelijke gegevensbank en de archieven verleend.

Er wordt in de memorie van toelichting evenwel meermaals uitgelegd dat het leesrecht altijd verbonden is aan het schrijfrecht.⁴¹

De gemachtigde van de minister heeft beaamd dat dit niet het geval is in het kader van artikel 16, dat dus een uitzondering vormt aangezien het paar "leesrecht/schrijfrecht" niet geldt voor de toezichthoudende organen, wier controlefunctie immers geen schrijfrecht vereist maar enkel een leesrecht.

De memorie van toelichting en de bespreking moeten dienovereenkomstig duidelijker worden geformuleerd.

Artikel 19

1. Doordat het zinsdeel "die een leesrecht en een schrijfrecht hebben" tussen komma's staat, moet het eerste lid zo worden gelezen dat niet alleen de basisdiensten maar ook de partnerdiensten noodzakelijkerwijze over die rechten beschikken.

Luidens artikel 17 komen die diensten echter pas in het bezit van die rechten als de Koning hun die verleent.

⁴¹ Zie bijvoorbeeld de inleidende bespreking van afdeling 5 van hoofdstuk 2 ("het leesrecht [gaat samen] met het schrijfrecht/de schrijfplicht") en de bespreking van artikel 17 ("de lees- en schrijfrechten [zijn] onlosmakelijk met elkaar verbonden").

Il y a donc lieu d'omettre cette virgule en manière telle que le texte soit dépourvu d'ambiguïté, à l'instar de la rédaction, *mutatis mutandis*, de l'article 23, alinéa 1^{er}, de l'avant-projet pour ce qui concerne le droit d'interrogation qui aurait été accordé aux services partenaires par le Roi.

2. Il est prévu que les services de base et les services partenaires qui bénéficient d'un droit de lecture et d'un droit d'écriture dans la banque de données commune T.E.R. sont tenus de consulter la banque de données et d'y introduire d'office leurs propres données à caractère personnel et les informations pertinentes, qui "proviennent des données à caractère personnel et [des] informations qui sont à [leur] disposition [...] dans le cadre de leurs missions respectives et des finalités qui y sont liées".

Or il ressort de l'article 18 que seul un service de base dispose d'un droit de création d'une "entité" dans la banque de données commune T.E.R.

Compte tenu de l'obligation pesant sur les services partenaires d'introduire dans la banque de données les données à caractère personnel et les informations dont ils disposent, il s'indiquera de préciser les modalités qui permettront à ces services d'être informés de la création d'une "entité" dans la banque de données. À défaut, les services concernés seraient confrontés à l'obligation de se tenir informés à leur initiative de l'éventualité de la création d'une "entité" à propos de laquelle ils disposeraient de données ou d'informations, ce qui, sur le plan pratique, ne saurait se concevoir que difficilement.

Article 30

Le commentaire de l'article 30 ne contient pas d'explication sur la portée du paragraphe 4, qui contient une nouvelle habilitation au Roi prévoyant qu'

"[il] peut par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, déterminer d'autres règles de responsabilité en matière de protection des données à caractère personnel des services de base et des services partenaires traitant ces données".

Interrogé à ce sujet, la déléguée du ministre a apporté les précisions suivantes:

"Un premier contrôle de qualité est opéré au sein même du service qui transmet une donnée ou une information à la [banque de données commune (BDC)] T.E.R. Les services disposant d'un droit de lecture et d'écriture dans la BDC doivent mettre en place un système de validation interne de leurs propres données afin d'avoir des données adéquates, pertinentes et non excessives au regard des missions et des finalités de la BDC (art. 14). L'article 15 prévoit qu'un service partenaire peut ajouter des données à propos d'une entité déjà enregistrée sans modifier/supprimer celles qui existent déjà. Seul le service qui a enregistré une donnée peut la modifier, la rectifier et la supprimer. Si un autre service estime qu'une donnée doit être modifiée, rectifiée ou supprimée, il en informe le service qui l'a enregistrée en vue de procéder le cas

Om alle dubbelzinnigheid in de tekst te voorkomen, moeten die komma's dus worden weggelaten, en dit, *mutatis mutandis*, naar het voorbeeld van de redactie van artikel 23, eerste lid, van het voorontwerp in verband met het vraagrecht dat door de Koning aan de partnerdiensten zou zijn verleend.

2. Er wordt bepaald dat de basisdiensten en de partnerdiensten die met betrekking tot de gemeenschappelijke gegevensbank T.E.R. over een schrijfrecht en een leesrecht beschikken, verplicht zijn de gegevensbank te raadplegen en ambtshalve daarin hun eigen persoonsgegevens en relevante informatie in te voeren, die "worden afgeleid uit de persoonsgegevens en informatie waarover [ze] beschikken in het kader van hun respectieve opdrachten en de daarmee verband houdende doeleinden".

Uit artikel 18 volgt echter dat alleen een basisdienst over een recht beschikt om een "entiteit" in de gemeenschappelijke gegevensbank T.E.R. te creëren.

Rekening houdend met het feit dat de partnerdiensten verplicht zijn om de persoonsgegevens en de informatie waarover ze beschikken, in de gegevensbank in te voeren, dienen de nadere regels te worden gespecificeerd op basis waarvan die diensten worden geïnformeerd zodra een "entiteit" in de gegevensbank wordt gecreëerd. Zo niet zouden de betrokken diensten zich verplicht zien op eigen initiatief op de hoogte te blijven van de eventuele creatie van een "entiteit" waarover ze gegevens en informatie zouden hebben, wat praktisch gezien maar moeilijk denkbaar zou zijn.

Artikel 30

De bespreking van artikel 30 bevat geen uitleg over de strekking van paragraaf 4, die de volgende nieuwe machtiging aan de Koning verleent:

"De Koning kan, bij een in Ministerraad overlegd besluit en na advies van de toezichthoudende overheden, andere regels bepalen inzake de verantwoordelijkheid op het gebied van de bescherming van persoonsgegevens van de basisdiensten en de partnerdiensten die deze gegevens verwerken."

Naar aanleiding van een vraag daarover heeft de gemachtigde van de minister de volgende preciseringen gegeven:

"Un premier contrôle de qualité est opéré au sein même du service qui transmet une donnée ou une information à la [banque de données commune (BDC)] T.E.R. Les services disposant d'un droit de lecture et d'écriture dans la BDC doivent mettre en place un système de validation interne de leurs propres données afin d'avoir des données adéquates, pertinentes et non excessives au regard des missions et des finalités de la BDC (art. 14). L'article 15 prévoit qu'un service partenaire peut ajouter des données à propos d'une entité déjà enregistrée sans modifier/supprimer celles qui existent déjà. Seul le service qui a enregistré une donnée peut la modifier, la rectifier et la supprimer. Si un autre service estime qu'une donnée doit être modifiée, rectifiée ou supprimée, il en informe le service qui l'a enregistrée en vue de procéder le

échéant aux adaptations nécessaires. En cas de désaccord, le responsable opérationnel prend la décision finale”.

Ces explications figureront utilement dans le commentaire de la disposition.

Articles 31 et 32

1. Aux termes de l'article 31 de l'avant-projet,

“[...] des données à caractère personnel et des informations enregistrées dans la banque de données commune T.E.R. ainsi que d'autres données à caractère personnel et informations pertinentes, y compris les informations classifiées au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, sont échangées au sein d'une ou de plusieurs plateformes de concertation créées auprès de chaque arrondissement judiciaire, appelée Task force locale, dénommée ci-après 'TFL', sauf si cet échange peut compromettre une enquête, l'exercice de l'action publique ou la sécurité de personnes”.

Il est prévu à l'article 32, § 1^{er}, alinéa 4, de l'avant-projet que le président de cette Task Force locale, en concertation avec ses “participants”, à savoir les services de renseignements et de sécurité, l'Organe de coordination pour l'analyse de la menace, la police fédérale, la police locale, la Direction générale de l'Office des étrangers du Service public fédéral Intérieur et le Ministère public,

“peut inviter d'autres services, organes ou instances en raison de la contribution qu'ils peuvent apporter par leur fonction ou leurs compétences à un suivi ciblé et individualisé de l'entité”.

Les articles 31 et 32 de l'avant-projet sont placés dans un chapitre 3 portant comme intitulé “Enrichissement des données relatives aux entités et suivi d'une entité validée dans la banque de données communes T.E.R.”.

2. Tel qu'il est libellé, le début de l'article 31 fait apparaître que l'échange de données au sein des Task Force locales a pour objectif

“d'assurer l'enrichissement des données à caractère personnel et informations relatives aux entités ainsi que le suivi et la prise de mesures à l'égard des entités validées dans la banque de données commune T.E.R.”.

Interrogée à ce sujet, la déléguée du ministre a précisé ce qui suit à propos de l'échange de données ou d'informations au sein de la Task force locale et de ce qu'il y avait lieu d'entendre quant à la notion d'enrichissement des données:

cas échéant aux adaptations nécessaires. En cas de désaccord, le responsable opérationnel prend la décision finale.”

Het verdient aanbeveling die toelichtingen in de bespreking van de bepaling op te nemen.

Artikelen 31 en 32

1. Luidens artikel 31 van het voorontwerp

“(…) worden er persoonsgegevens en informatie uit de gemeenschappelijke gegevensbank T.E.R., alsook andere persoonsgegevens en relevante informatie, waaronder geclassificeerde informatie in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmaatregelen, veiligheidsattesten en veiligheidsadviezen, uitgewisseld binnen een of meer overlegplatformen die bij elk gerechtelijk arrondissement zijn opgericht, onder de naam ‘Lokale task force’ (hierna ‘LTF’), tenzij die uitwisseling een onderzoek, de uitoefening van de strafvordering of de veiligheid van personen in het gedrang kan brengen.”

In artikel 32, § 1, vierde lid, van het voorontwerp wordt bepaald dat de voorzitter van die lokale taskforce in overleg met zijn “deelnemers”, te weten de inlichtingen- en veiligheidsdiensten, het Coördinatieorgaan voor de dreigingsanalyse, de federale politie, de lokale politie, de Algemene Directie Dienst Vreemdelingenzaken van de Federale overheidssdienst Binnenlandse Zaken en het Openbaar Ministerie,

“andere diensten, organen of instanties [kan] uitnodigen wegens de bijdrage die ze door hun functie of bevoegdheden kunnen leveren aan een gerichte en geïndividualiseerde opvolging van de entiteit.”

De artikelen 31 en 32 van het voorontwerp zijn ondergebracht in een hoofdstuk 3 met als opschrift “Verrijking van gegevens over entiteiten en opvolging van een in de gemeenschappelijke gegevensbank T.E.R. gevalideerde entiteit”.

2. Uit de redactie van het begin van artikel 31 kan worden opgemaakt dat de uitwisseling van gegevens binnen de lokale taskforce het volgende doel zou dienen:

“de verrijking van persoonsgegevens en informatie over entiteiten en de opvolging en het nemen van maatregelen ten aanzien van de in de gemeenschappelijke gegevensbank T.E.R.”

Naar aanleiding van een vraag daarover heeft de gemachtigde van de minister het volgende gesteld over de uitwisseling van gegevens of informatie binnen de lokale taskforce en over wat dient te worden verstaan onder het begrip “verrijking van gegevens”:

“L’avant-projet de loi utilise en effet à plusieurs reprises la notion d’enrichissement des données/informations. Cette notion doit être comprise d’une part comme une contextualisation des données et d’autre part comme la mise à jour de l’information déjà enregistrée et/ou l’ajout des informations nouvelles.

Pourquoi faut-il contextualiser?

La [banque de données T.E.R.] ne contient pas toutes les informations disponibles des services de base ou des services partenaires sur les entités (la [banque de données T.E.R.] ne reprend pas, par exemple, le contenu *in extenso* des procès-verbaux) et la contextualisation permet donc de donner tout le contexte relatif à la donnée enregistrée dans la [banque de données T.E.R.] (personne, véhicule, ...).

Pourquoi faut-il mettre à jour?

Lors de la [Task force locale] et de la discussion avec les différents services présents, il peut ressortir qu’il y ait des nouvelles données à enregistrer et qu’il faille donc ‘enrichir’ la banque de données ou qu’il soit nécessaire de mettre de l’information déjà enregistrées à jour.

Telles qu’elles sont définies à l’article 2, 5° et 6°, de l’avant-projet, les données à caractère personnel et les informations qui peuvent être insérées dans la banque de données commune T.E.R. sont des données et des informations non classifiées.

[...]

Comme l’article 2, points [5]° et [6]°, le prévoit, la [banque de données T.E.R.] ne contient pas de données classifiées. Utiliser une banque de données qui peut contenir des données classifiées a des implications majeures en termes de développement, sécurité de la banque de données, ce qui n’est pas le cas de la banque de données commune T.E.R.

Lors des réunions des [Task forces locales], dans le cadre de l’enrichissement des données, entre partenaires qui disposent d’une habilitation de sécurité et du besoin d’en connaître, des informations classifiées sur une personne enregistrée dans la banque de données T.E.R. peuvent être échangées”.

Il ressort des explications ainsi fournies que l’échange de données au sein de la Task force locale peut amener à préciser des données à caractère personnel ou des informations qui sont déjà contenues dans la banque de données commune T.E.R., à mettre à jour ces données ou à en introduire de nouvelles.

Toutefois, compte tenu des définitions prescrites par les 5° et 6° de l’article 2 de l’avant-projet, et afin d’assurer la cohérence de l’ensemble du dispositif, l’article 31 de l’avant-projet ne pourrait être interprété comme permettant l’enregistrement dans la banque de données commune T.E.R. de données ou d’informations classifiées, celles-ci pouvant tout au plus faire l’objet d’échanges lors des réunions de la Task force locale.

“L’avant-projet de loi utilise en effet à plusieurs reprises la notion d’enrichissement des données/informations. Cette notion doit être comprise d’une part comme une contextualisation des données et d’autre part comme la mise à jour de l’information déjà enregistrée et/ou l’ajout des informations nouvelles.

Pourquoi faut-il contextualiser?

La [banque de données T.E.R.] ne contient pas toutes les informations disponibles des services de base ou des services partenaires sur les entités (la [banque de données T.E.R.] ne reprend pas, par exemple, le contenu *in extenso* des procès-verbaux) et la contextualisation permet donc de donner tout le contexte relatif à la donnée enregistrée dans la [banque de données T.E.R.] (personne, véhicule, ...).

Pourquoi faut-il mettre à jour?

Lors de la [Task force locale] et de la discussion avec les différents services présents, il peut ressortir qu’il y ait des nouvelles données à enregistrer et qu’il faille donc ‘enrichir’ la banque de données ou qu’il soit nécessaire de mettre de l’information déjà enregistrées à jour.

Telles qu’elles sont définies à l’article 2, 5° et 6°, de l’avant-projet, les données à caractère personnel et les informations qui peuvent être insérées dans la banque de données commune T.E.R. sont des données et des informations non classifiées.

(...)

Comme l’article 2, points [5]° et [6]°, le prévoit, la [banque de données T.E.R.] ne contient pas de données classifiées. Utiliser une banque de données qui peut contenir des données classifiées a des implications majeures en termes de développement, sécurité de la banque de données, ce qui n’est pas le cas de la banque de données commune T.E.R.

Lors des réunions des [Task forces locales], dans le cadre de l’enrichissement des données, entre partenaires qui disposent d’une habilitation de sécurité et du besoin d’en connaître, des informations classifiées sur une personne enregistrée dans la banque de données T.E.R. peuvent être échangées.”

Uit die toelichtingen blijkt dat de gegevensuitwisseling binnen de lokale taskforce kan leiden tot een precisering van persoonsgegevens of informatie die al in de gemeenschappelijke gegevensbank T.E.R. zitten, tot een update van die gegevens of tot de invoering van nieuwe gegevens.

Gelet op de definities in de punten 5° en 6° van artikel 2 van het voorontwerp, mag, teneinde de samenhang van het hele dispositief te bewaren, artikel 31 van het voorontwerp evenwel niet aldus worden geïnterpreteerd dat geclassificeerde gegevens of geclassificeerde informatie in de gemeenschappelijke gegevensbank T.E.R. kunnen worden geregistreerd. Die gegevens en informatie mogen hoogstens tijdens vergaderingen van de lokale taskforce worden uitgewisseld.

Sous réserve de cette interprétation, l'article 31 de l'avant-projet est admissible.

3. Interrogée quant à la portée de l'article 32, § 1^{er}, alinéa 4, en projet, la déléguée du ministre a également apporté les précisions qui suivent:

“Lors des réunions de la [Task Force locale], les principes de base (chapitre 2 sections 5 et 7) contenus dans le projet de loi en matière d'accès ou de communication de données sont respectés.

Chaque membre présent travaille sur la base du principe du besoin d'en connaître.

Si un membre externe est invité, il est présent dans le but exclusif de fournir des données, éclairer un point précis par son expertise et pas pour recevoir des données. Il est présent pour ‘son point’ et quitte ensuite la réunion après son exposé”.

Il résulte de ces explications que l'article 32, § 1^{er}, alinéa 4, en projet doit être interprété comme permettant aux “autres services, organes ou instances” invités à participer aux réunions de la Task force locale de communiquer des données ou des informations dont ils seraient détenteurs en raison de leur mission en vue d'enrichir les données ou informations contenues dans la banque de données. Ils ne pourraient en revanche se voir communiquer des données ou informations dont les autres membres de la Task force locale seraient détenteurs.

C'est ici encore sous réserve de cette interprétation que l'article 32 de l'avant-projet est admissible.

Article 32

L'article 32, § 1^{er}, prévoit la composition de la “Task force locale”, dénommée TFL.

Cependant, il n'y a pas d'indication quant au nombre de membres par catégories ni quant aux modalités de fonctionnement de celle-ci.

Interrogée à cet égard, la déléguée du ministre a répondu ce qui suit:

“Le texte va être réexaminé pour prévoir éventuellement la présence au minimum d'une personne par autorité présente à la TLF. Le texte va être réexaminé pour prévoir éventuellement un nombre minimum de réunion par an”.

Articles 34 à 49

Comme en a convenu la déléguée du ministre, l'exposé des motifs et le commentaire seront complétés par une explication article par article des dispositions en projet afin d'expliquer les modifications qui sont apportées à la loi du 30 juillet 2018.

Onder voorbehoud van die interpretatie is artikel 31 van het voorontwerp toelaatbaar.

3. Naar aanleiding van een vraag over de strekking van het ontworpen artikel 32, § 1, vierde lid, heeft de gemachtigde van de minister ook de volgende preciseringen gegeven:

“Lors des réunions de la [Task Force locale], les principes de base (chapitre 2 sections 5 et 7) contenus dans le projet de loi en matière d'accès ou de communication de données sont respectés.

Chaque membre présent travaille sur la base du principe du besoin d'en connaître.

Si un membre externe est invité, il est présent dans le but exclusif de fournir des données, éclairer un point précis par son expertise et pas pour recevoir des données. Il est présent pour ‘son point’ et quitte ensuite la réunion après son exposé.”

Uit die toelichtingen volgt dat het ontworpen artikel 32, § 1, vierde lid, zo moet worden geïnterpreteerd dat “andere diensten, organen of instanties” die zijn uitgenodigd om deel te nemen aan de vergaderingen van de lokale taskforce, gegevens of informatie die ze in het kader van hun opdracht bezitten, kunnen meedelen om de gegevens of de informatie die al in de gegevensbank zitten, te verrijken. Ze zouden daarentegen geen gegevens of informatie kunnen ontvangen die de andere leden van de lokale taskforce zouden bezitten.

Onder voorbehoud van die interpretatie is ook artikel 32 van het voorontwerp toelaatbaar.

Artikel 32

Artikel 32, § 1, regelt de samenstelling van de lokale taskforce, die LTF wordt genoemd.

Er wordt echter niets bepaald in verband met het aantal leden per categorie, noch in verband met de nadere regels voor de werkwijze van die LTF.

Op een vraag daarover heeft de gemachtigde van de minister het volgende geantwoord:

“Le texte va être réexaminé pour prévoir éventuellement la présence au minimum d'une personne par autorité présente à la TLF. Le texte va être réexaminé pour prévoir éventuellement un nombre minimum de réunion par an.”

Artikelen 34 tot 49

Zoals de gemachtigde van de minister heeft beaamd, moeten de memorie van toelichting en de bespreking worden aangevuld met een artikelsgewijze uitleg van de ontworpen bepalingen, zodat de wijzigingen die in de wet van 30 juli 2018 worden aangebracht, worden toegelicht.

Article 46

L'article 46 tend à compléter l'article 162 de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard de traitement de données à caractère personnel' par deux alinéas nouveaux, formant les alinéas 3 et 4.

Il résulte de l'alinéa 3 en projet que, par dérogation à l'alinéa 1^{er} actuel de l'article 162, la consultation de données à caractère personnel relatives aux entités enregistrées dans la banque de données commune T.E.R. par un responsable du traitement ultérieur, à des fins historiques, scientifiques ou statistiques, est autorisée par le responsable opérationnel de la banque de données après concertation avec les services de base.

La question se pose de savoir pour quel motif une telle dérogation est apportée à l'article 162, alinéa 1^{er}, de la loi précitée en ne prévoyant pas une réserve à l'autorisation de consultation dans l'hypothèse où cette dernière nuirait à l'exercice de l'action publique, à la sécurité d'une personne ou à la relation avec un service répressif d'un État étranger, cette réserve étant d'ailleurs également prévue par l'article 20 de l'avant-projet.

À défaut de justification sur ce point, le dispositif sera complété afin d'envisager cette hypothèse.

Par ailleurs, dans la version néerlandaise de l'alinéa 3, il y a lieu d'insérer le verbe "toestaan" entre le mot "entiteiten" et les mots "door de operationeel verantwoordelijke".

Article 54

Comme en a convenu la déléguée du ministre, il y a lieu de compléter l'alinéa 2, *in fine*, afin de prévoir que le Roi puisse remplacer les références existantes dans les lois aux dispositions des arrêtés royaux abrogés par les références aux dispositions correspondantes "de la présente loi ou de ses arrêtés d'exécution".

Article 56

L'article 56 est rédigé de la manière suivante:

"La présente loi entre en vigueur à la date fixée par le Roi et au plus tard le xx/xx/xxxx".

Interrogée sur le fait que la date ultime d'entrée en vigueur n'est pas complétée dans l'avant-projet, la déléguée du ministre a précisé ce qui suit:

"Il était en effet important que la loi et l'arrêté royal portant exécution de celle-ci entrent en vigueur en même temps, et ce, pour permettre une application complète de la législation

Artikel 46

Artikel 46 strekt ertoe artikel 162 van de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens' aan te vullen met twee nieuwe leden, die het derde en het vierde lid worden.

Uit het ontworpen derde lid vloeit voort dat, in afwijking van het huidige eerste lid van artikel 162, de operationeel verantwoordelijke van de gegevensbank na overleg met de basisdiensten kan toestaan dat een verantwoordelijke voor verdere verwerking persoonsgegevens betreffende entiteiten die in de gemeenschappelijke gegevensbank T.E.R. geregistreerd staan, raadpleegt voor historische, wetenschappelijke of statistische doeleinden.

De vraag rijst waarom in een dergelijke afwijking van artikel 162, eerste lid, van de voornoemde wet wordt voorzien, zonder dat ten aanzien van de toestemming tot raadpleging een voorbehoud wordt gemaakt voor het geval dat die raadpleging de uitoefening van de strafvordering, de veiligheid van een persoon of de relatie met een rechtshandhavingsautoriteit van een buitenlandse Staat in het gedrang zou brengen. Dat voorbehoud wordt overigens ook in artikel 20 van het voorontwerp gemaakt.

Als er dienaangaande geen verantwoording kan worden gegeven, moet het dispositief worden aangevuld zodat in dat geval wordt voorzien.

In de Nederlandse tekst van het derde lid dient overigens het woord "toestaan" ingevoegd te worden tussen het woord "entiteiten" en de woorden "door de operationeel verantwoordelijke".

Artikel 54

Zoals de gemachtigde van de minister heeft beaamd, dient het tweede lid, *in fine*, te worden aangevuld zodat bepaald wordt dat de Koning de bestaande verwijzingen in de wetten naar de bepalingen van de opgeheven koninklijke besluiten kan vervangen door verwijzingen naar de ermee overeenstemmende bepalingen "van deze wet of van de besluiten tot uitvoering ervan".

Artikel 56

Artikel 56 is als volgt geredigeerd:

"Deze wet treedt in werking op de datum bepaald door de Koning en uiterlijk op xxx."

Naar aanleiding van een vraag over het feit dat het voorontwerp de uiterste inwerkingtredingsdatum onvermeld laat, heeft de gemachtigde van de minister het volgende gesteld:

"Il était en effet important que la loi et l'arrêté royal portant exécution de celle-ci entrent en vigueur en même temps, et ce, pour permettre une application complète de la législation

en matière de la [banque de données communes] T.E.R. Le but est que le projet de loi et d'arrêté royal entrent en vigueur encore sous cette législature. Nous proposons donc de prendre une date ultime (et au plus tard) fin 2024".

La date sera complétée dans l'article 56 conformément aux règles de légistique sur ce point⁴². Par voie de conséquence, le commentaire contiendra une explication du choix de cette entrée en vigueur.

OBSERVATIONS FINALES

L'avant-projet sera revu sur les points suivants:

– à l'article 2, 5°, il y a lieu de reproduire l'intitulé complet du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 'relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)', de préciser qu'il est abrégé en "RGPD" et d'utiliser cette abréviation pour la suite de l'avant-projet;

– de même dans la version française de l'article 33, § 2, 6°, il y a lieu de reproduire l'intitulé exact de la loi du 18 septembre 2017 'relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces';

– dans la version française de l'article 2, 15°, il y a lieu de supprimer le doublon du mot "organique";

– à l'article 6, § 2, alinéa 1^{er}, 1), c), i., de la version française, il y a lieu d'omettre le mot "de".

– enfin, les renvois d'articles doivent être vérifiés ou précisés, comme par exemple dans les articles 7, § 2, alinéa 3, 4°, 11, alinéa 2, 5°, 16, 39, 44 et 50; il en va de même pour l'article 32, § 1^{er}, alinéa 3, qui contient une erreur de renvoi car il y a lieu d'y viser l'article 4, alinéa 3, de la loi du 11 décembre 1998 'relative à la classification et aux habilitations, attestations et avis de sécurité' et pour l'article 32, § 2, alinéa 1^{er}, 1°, qui doit renvoyer à l'article 31 et non à l'article 32 de l'avant-projet.

*

Le greffier,

Esther CONTI

Le président,

Pierre VANDERNOOT

⁴² *Principes de technique législative – Guide de rédaction des textes législatifs et réglementaires*, www.raadvst-consetat.be, onglet "Technique législative", recommandations n^{os} 154.1 à 154.1.2 et formule F 4-5-2-4.

en matière de la [banque de données communes] T.E.R. Le but est que le projet de loi et d'arrêté royal entrent en vigueur encore sous cette législature. Nous proposons donc de prendre une date ultime (et au plus tard) fin 2024."

Overeenkomstig de desbetreffende regels van de wetgevingstechniek dient de datum in artikel 56 te worden aangevuld.⁴² Dientengevolge moet de keuze van die datum van inwerking-treding in de bespreking van het artikel worden toegelicht.

SLOTOPMERKINGEN

Het voorontwerp moet op de volgende punten worden herzien:

– in artikel 2, 5°, dient het volledige opschrift te worden vermeld van verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 'betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)'; ook dient te worden vermeld dat dat opschrift wordt afgekort als "AVG" en dient die afkorting in het vervolg van het voorontwerp te worden gebruikt;

– Enzo moet in de Franse tekst van artikel 33, § 2, 6°, het juiste opschrift van de wet van 18 september 2017 'relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces' worden opgegeven;

– in de Franse tekst van artikel 2, 15°, moet de eerste vermelding van het woord "organique" worden geschrapt;

– in de Franse tekst van artikel 6, § 2, eerste lid, 1°, 1), c), i., dient het woord "de" te worden weggelaten;

– ten slotte dienen de verwijzingen naar artikelen te worden gecontroleerd of gepreciseerd, zoals bijvoorbeeld in de artikelen 7, § 2, derde lid, 4°, 11, tweede lid, 5°, 16, 39, 44 en 50; hetzelfde geldt voor artikel 32, § 1, derde lid, dat een verkeerde verwijzing bevat aangezien daarin dient te worden verwezen naar artikel 4, derde lid, van de wet van 11 december 1998 'betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst', en voor artikel 32, § 2, eerste lid, 1°, dat naar artikel 31 en niet naar artikel 32 van het voorontwerp moet verwijzen.

*

De griffier,

Esther CONTI

De voorzitter,

Pierre VANDERNOOT

⁴² *Beginnelsen van de wetgevingstechniek – Handleiding voor het opstellen van wetgevende en reglementaire teksten*, www.raadvst-consetat.be, tab "Wetgevingstechniek", aanbevelingen 154.1 en 154.1.2 en formule F 4-5-2-4.

PROJET DE LOI

PHILIPPE,

ROI DES BELGES,

À tous, présents et à venir,

SALUT.

Sur la proposition du ministre de la Justice et de la ministre de l'Intérieur,

NOUS AVONS ARRÊTÉ ET ARRÊTONS:

Le ministre de la Justice et la ministre de l'Intérieur sont chargés de présenter en notre nom à la Chambre des représentants le projet de loi dont la teneur suit:

CHAPITRE 1^{ER}**Dispositions générales****Article 1^{er}**

La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2

Pour l'application de la présente loi et de ses arrêtés d'exécution, il faut entendre par:

1° "loi relative à la protection des données": la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel;

2° "services de base": l'Organe de la coordination pour l'analyse de la menace, la police intégrée et les services de renseignement et de sécurité;

3° "services partenaires":

a) l'Unité d'information des passagers du Centre de Crise national du Service Public fédéral Intérieur;

b) la Direction générale Sécurité et Prévention du Service Public fédéral Intérieur;

WETSONTWERP

FILIP,

KONING DER BELGEN,

Aan allen die nu zijn en hierna wezen zullen,

ONZE GROET.

Op de voordracht van de minister van Justitie en de minister van Binnenlandse Zaken,

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

De minister van Justitie en de minister van Binnenlandse Zaken zijn ermee belast in onze naam bij de Kamer van volksvertegenwoordigers het ontwerp van wet in te dienen waarvan de tekst hierna volgt:

HOOFDSTUK 1**Algemene bepalingen****Artikel 1**

Deze wet regelt een aangelegenheid zoals bedoeld in artikel 74 van de Grondwet.

Art. 2

Voor de toepassing van deze wet en de uitvoeringsbesluiten ervan wordt verstaan onder:

1° "wet gegevensbescherming": de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens;

2° "basisdiensten": het Coördinatieorgaan voor de dreigingsanalyse, de geïntegreerde politie, de inlichtingen- en veiligheidsdiensten;

3° "partnerdiensten":

a) de Passagiersinformatie-eenheid van de Nationaal Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken;

b) de Algemene Directie Veiligheid en Preventie van de Federale Overheidsdienst Binnenlandse Zaken;

c) la Direction générale des Etablissements Pénitentiaires du Service Public fédéral Justice;

d) la Direction générale Affaires Consulaires du Service Public fédéral Affaires étrangères;

e) le Ministère public;

f) la Cellule de Traitement des Informations Financières;

g) la Direction générale de l'Office des Etrangers du Service Public fédéral Intérieur;

h) l'Administration générale des douanes et accises du Service Public fédéral Finances;

i) le Service des cultes et de la laïcité du Service Public fédéral Justice;

a) l'Autorité Nationale de Sécurité;

b) l'Administration générale de la Trésorerie du Service Public fédéral Finances;

c) dans le cadre de leurs missions légales d'accompagnement judiciaire et de la surveillance d'auteurs d'infractions, l'Administration générale des Maisons de Justice de la Communauté Française, le département Maison de Justice du Ministère de la Communauté Germanophone, l'Agence flamande pour la Justice et le Maintien, l'Administration générale de l'Aide à la Jeunesse de la Communauté Française, le département Aide à la Jeunesse de la Communauté Germanophone et l'Agence flamande Opgroeien;

4° "entité":

a) "entité validée": toute personne physique majeure ou mineure de douze ans et plus, toute personne morale ou association de fait qui répond aux critères d'un *foreign terrorist fighter*, *homegrown terrorist fighter*, extrémiste potentiellement violent, d'une personne condamnée pour terrorisme ou d'un propagandiste de haine, ainsi que l'ensemble des moyens utilisés par celles-ci;

b) "entité en pré-enquête": toute personne physique majeure ou mineure de douze ans et plus, toute personne morale ou association de fait à propos de laquelle il existe des indices sérieux qu'elle puisse remplir les critères d'un *foreign terrorist fighter*, *homegrown terrorist fighter*, extrémiste potentiellement violent ou d'un propagandiste de haine, ainsi que l'ensemble des moyens utilisés par celles-ci;

c) het Directoraat-generaal Penitentiaire Inrichtingen van de Federale Overheidsdienst Justitie;

d) het Directoraat-generaal Consulaire Zaken van de Federale Overheidsdienst Buitenlandse Zaken;

e) het Openbaar Ministerie;

f) de Cel voor Financiële Informatieverwerking;

g) de Algemene Directie Dienst Vreemdelingenzaken van de Federale Overheidsdienst Binnenlandse Zaken;

h) de Algemene Administratie van de douane en accijnzen van de Federale Overheidsdienst Financiën;

i) de Dienst zrediensten en vrijzinnigheid van de Federale Overheidsdienst Justitie;

j) de Nationale Veiligheidsoverheid;

k) de Algemene Administratie van de Thesaurie van de Federale Overheidsdienst Financiën;

l) In het kader van hun wettelijke opdrachten van justitiële begeleiding van en toezicht op daders van misdrijven, de Algemene Administratie van Justitiehuisen van de Franse Gemeenschap, het departement Justitiehuis van het Ministerie van de Duitstalige gemeenschap, het Vlaams Agentschap Justitie en Handhaving, de Algemene Administratie van de hulpverlening aan de jeugd van de Franse Gemeenschap, het departement Jeugdbijstand van de Duitstalige gemeenschap en het Vlaams Agentschap Opgroeien;

4° "entiteit":

a) "gevalideerde entiteit": elke meerderjarige natuurlijke persoon of minderjarige natuurlijke persoon van twaalf jaar en ouder, elke rechtspersoon of feitelijke vereniging die beantwoordt aan de criteria van een *foreign terrorist fighter*, *homegrown terrorist fighter*, potentieel gewelddadige extremist, terrorismeveroordeelde of haatpropagandist, alsook alle de door hen aangewende middelen;

b) "entiteit in vooronderzoek": elke meerderjarige natuurlijke persoon of minderjarige natuurlijke persoon van twaalf jaar en ouder, elke rechtspersoon of feitelijke vereniging ten aanzien waarvan er ernstige aanwijzingen bestaan dat ze kan voldoen aan de criteria van een *foreign terrorist fighter*, *homegrown terrorist fighter*, potentieel gewelddadige extremist of haatpropagandist, alsook alle de door hen aangewende middelen;

5° “groupements terroristes”: les groupements organisant ou soutenant des activités terroristes;

6° “zone de conflit djihadiste”: le territoire en proie à une lutte livrée afin de propager, d'imposer ou de protéger de manière violente une vision de la religion islamique et qui est défini par le Conseil national de sécurité sur proposition du responsable du traitement des données de la banque de données commune T.E.R. sur base de l'analyse stratégique effectuée par l'Organe de coordination pour l'analyse de la menace;

7° “foreign terrorist fighters”: les personnes physiques résidant en Belgique ou ayant résidé en Belgique, ayant ou non la nationalité belge et qui, dans le but de se rallier à des groupements terroristes ou de leur fournir un soutien actif ou passif, se trouvent dans l'une des situations suivantes:

a) elles se sont rendues dans une zone de conflit djihadiste;

b) elles ont quitté la Belgique pour se rendre dans une zone de conflit djihadiste;

c) elles sont en route vers la Belgique ou sont revenues en Belgique après s'être rendues dans une zone de conflit djihadiste;

d) elles ont, volontairement ou involontairement, été empêchées de se rendre dans une zone de conflit djihadiste;

e) elles ont l'intention de se rendre dans une zone de conflit djihadiste à la condition que des indications sérieuses démontrent cette intention;

8° “homegrown terrorist fighters”: les personnes physiques qui ont un lien avec la Belgique et pour lesquelles au minimum une des conditions suivantes est remplie:

a) il existe des indications sérieuses qu'elles ont l'intention de recourir à la violence à l'encontre de personnes ou d'intérêts matériels, pour des motifs idéologiques ou politiques, dans le but d'atteindre leurs objectifs par la terreur, l'intimidation ou les menaces;

b) il existe des indications sérieuses qu'elles donnent intentionnellement un soutien, notamment logistique, financier, ou aux fins de formation ou recrutement, aux personnes visées au a), ou aux personnes enregistrées en tant que *foreign terrorist fighters* conformément au 7°

5° “terroristische groeperingen”: de groeperingen die terroristische activiteiten organiseren of er steun aan verlenen;

6° “jihadistische conflictzone”: het grondgebied waarop strijd geleverd wordt om een stellingname binnen het islamitische geloof op een gewelddadige manier te propageren, op te leggen of te beschermen, dat wordt afgebakend door de Nationale Veiligheidsraad op voorstel van de verantwoordelijke voor de verwerking van gegevens uit de gemeenschappelijke gegevensbank T.E.R. op basis van de strategische analyse die werd uitgevoerd door het Coördinatieorgaan voor de dreigingsanalyse;

7° “foreign terrorist fighter”: de natuurlijke personen die in België verblijven of verbleven hebben, die al dan niet de Belgische nationaliteit bezitten en die zich, met het oog om zich bij terroristische groeperingen aan te sluiten of deze actief of passief steun te verlenen, in een van de volgende situaties bevinden:

a) ze zijn naar een jihadistische conflictzone afgereisd;

b) ze hebben België verlaten om naar een jihadistische conflictzone af te reizen;

c) ze zijn naar België onderweg of naar België teruggekeerd na afgereisd te zijn naar een jihadistische conflictzone;

d) ze werden gewild of ongewild verhinderd om naar een jihadistische conflictzone af te reizen;

e) ze hebben de intentie om naar een jihadistische conflictzone af te reizen, op voorwaarde dat deze intentie aangetoond wordt door ernstige aanwijzingen;

8° “homegrown terrorist fighters”: de natuurlijke personen die een band hebben met België en voor wie aan ten minstens één van de volgende criteria is voldaan:

a) er bestaan ernstige aanwijzingen dat zij de intentie hebben om geweld te gebruiken tegen personen of materiële belangen om ideologische of politieke redenen met het doel hun doelstellingen door middel van terreur, intimidatie of dreigingen te bereiken;

b) er bestaan ernstige aanwijzingen dat zij doelbewust steun leveren, onder meer logistiek, financieel of met opleidings- of rekruteringsdoeleinden, aan de personen geïdentificeerd in a), of aan personen die geregistreerd staan als *foreign terrorist fighter* zoals bedoeld in de bepaling

pour lesquelles il existe des indications sérieuses qu'elles ont l'intention de commettre un acte violent;

9° “extrémistes potentiellement violents”: les personnes physiques qui ont un lien avec la Belgique et qui remplissent les critères cumulatifs suivants:

a) elles ont des conceptions extrémistes qui justifient l'usage de la violence ou de la contrainte comme méthode d'action en Belgique;

b) il existe des indications fiables qu'elles ont l'intention de recourir à la violence, et ce en relation avec les conceptions mentionnées en a);

c) elles répondent au minimum à une des conditions suivantes augmentant le risque de violence:

i. elles entretiennent systématiquement des contacts sociaux au sein de milieux extrémistes;

ii. elles ont des problèmes psychiques constatés par un professionnel compétent en la matière;

iii. elles ont commis des actes ou présentent des antécédents qui peuvent être considérés comme soit a) un crime ou un délit portant atteinte à ou menaçant l'intégrité physique ou psychique de tiers; soit b) des instructions ou des formations relatives à la fabrication ou l'utilisation d'explosifs, d'armes à feu ou d'autres armes ou substances nocives ou dangereuses, ou pour d'autres méthodes et techniques spécifiques en vue de commettre des infractions terroristes conformément à l'article 137 du Code pénal; soit c) des agissements en connaissance de cause constituant un soutien matériel en faveur d'une organisation ou d'un réseau terroriste/extrémiste; soit d) des agissements dont la nature indique un niveau de vigilance préoccupant de l'individu à l'égard de la sécurité.;

10° “personnes condamnées pour terrorisme”: les personnes physiques qui ont un lien avec la Belgique et qui remplissent les deux critères cumulatifs suivants:

a)

i. elles ont été condamnées par un jugement ou un arrêt passé en force de chose jugée pour une infraction terroriste visée au Livre II, Titre I^{ter} du Code Pénal ou elles ont été condamnées à l'étranger par un jugement ou un arrêt passé en force de chose jugée pour des faits qui peuvent être qualifiés d'infractions terroristes visées au Livre II, Titre I^{ter} du Code Pénal ou,

ou 7° en waarvoor er ernstige aanwijzingen bestaan dat zij de intentie hebben om een gewelddadige actie uit te voeren;

9° “potentieel gewelddadige extremisten”: de natuurlijke personen die een aanknopingspunt met België hebben en die voldoen aan volgende cumulatieve criteria:

a) ze hebben extremistische opvattingen die het gebruik van geweld of dwang als actiemethode in België legitimeren;

b) er zijn betrouwbare aanwijzingen dat ze de intentie hebben om geweld te gebruiken, en dit in verband met de opvattingen vermeld in a);

c) ze voldoen aan minstens een van de volgende criteria die het risico op geweldpleging verhogen:

i. ze hebben systematisch sociale contacten binnen extremistische milieus;

ii. ze hebben een psychische problematiek, vastgesteld door een daartoe gekwalificeerde deskundige;

iii. ze pleegden daden of stelden anteceden ten die beschouwd kunnen worden als ofwel a) een misdaad of wanbedrijf die de fysieke of psychische integriteit van derden aantast of bedreigt; ofwel b) onderrichtingen of een opleiding voor de vervaardiging of het gebruik van explosieven, vuurwapens of andere wapens of schadelijke of gevaarlijke stoffen, dan wel voor andere specifieke methoden en technieken nuttig voor het plegen van terroristische misdrijven bedoeld in artikel 137 van het Strafwetboek, ofwel c) bewuste handelingen die als materiële steun voor een terroristische/extremistische organisatie of netwerk gelden; ofwel d) feiten die door hun aard wijzen op een verontrustend veiligheidsbewustzijn in hoofde van de betrokkene.

10° “terrorismeveroordeelden”: de natuurlijke personen die een aanknopingspunt hebben met België en die voldoen aan de volgende twee cumulatieve criteria:

a)

i. ze werden veroordeeld door een in kracht van gewijsde getreden vonnis of arrest voor een terroristisch misdrijf bedoeld in Boek II, Titel I^{ter} van het Strafwetboek of ze werden in het buitenland veroordeeld door een in kracht van gewijsde getreden vonnis of arrest voor feiten die gekwalificeerd kunnen worden als terroristische misdrijven bedoeld in Boek II, Titel I^{ter} van het Strafwetboek of,

ii. elles ont fait l'objet d'une mesure de protection passée en force de chose jugée prise par un tribunal de jeunesse ou une Cour pour des faits qualifiés d'infractions terroristes visées au Livre II, Titre I^{ter} du Code Pénal ou elles ont fait l'objet d'une telle mesure ou ont été condamnées définitivement à l'étranger pour des faits qui peuvent être qualifiés d'infraction terroriste sur la base du Livre II, Titre I^{ter} du Code Pénal ou,

iii. elles ont fait l'objet d'une décision judiciaire d'internement passée en force de chose jugée, pour une infraction terroriste visée au Livre II, Titre I^{ter} du Code Pénal, ou ont fait l'objet d'une telle mesure à l'étranger pour des faits qui peuvent être qualifiés d'infraction terroriste sur la base du Livre II, Titre I^{ter} du Code Pénal;

b) l'Organe de coordination pour l'analyse de la menace leur a attribué un niveau de la menace "Niveau 2 ou MOYEN", "Niveau 3 ou GRAVE" ou "Niveau 4 ou TRÈS GRAVE" conformément à l'article 6, paragraphe 1^{er}, de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace;

11° "propagandistes de haine": les personnes physiques ou morales, associations de fait, y compris l'ensemble des moyens utilisés par celles-ci, nonobstant leur nationalité, lieu de résidence ou siège, qui remplissent les critères cumulatifs suivants:

a) ont pour objectif de porter atteinte aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux autres fondements de l'État de droit;

b) justifient l'usage de la violence ou de la contrainte comme moyen d'action;

c) propagent leurs convictions aux autres en vue d'exercer une influence radicalisante; on entend par "influence radicalisante": toute action exercée par une entité dans le but d'initier, de soutenir ou de contribuer à un processus de radicalisation au sens de l'article 3, 15°, de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité;

d) ont un lien avec la Belgique;

12° "données à caractère personnel": les données à caractère personnel au sens de l'article 4, 1), du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes

ii. ze hebben het voorwerp uitgemaakt van een in kracht van gewijsde getreden beschermingsmaatregel opgelegd door een jeugdrechtbank of een Hof voor feiten gekwalificeerd als terroristische misdrijven bedoeld in Boek II, Titel I^{ter} van het Strafwetboek of ze hebben het voorwerp uitgemaakt van zo'n maatregel of ze werden definitief veroordeeld in het buitenland voor feiten die gekwalificeerd kunnen worden als een terroristisch misdrijf bedoeld in Boek II, Titel I^{ter} van het Strafwetboek of,

iii. ze hebben het voorwerp uitgemaakt van een gerechtelijke beslissing tot internering dewelke in kracht van gewijsde is getreden voor een terroristische misdrijf bedoeld in Boek II, Titel I^{ter} van het Strafwetboek, of ze hebben het voorwerp uitgemaakt van zo'n maatregel in het buitenland voor feiten die gekwalificeerd kunnen worden als een terroristisch misdrijf bedoeld in Boek II, Titel I^{ter} van het Strafwetboek;

b) zij kregen door het Coördinatieorgaan voor de dreigingsanalyse een niveau van de dreiging toegekend van "Niveau 2 of GEMIDDELD", "Niveau 3 of ERNSTIG" of "Niveau 4 of ZEER ERNSTIG" overeenkomstig artikel 6, paragraaf 1 van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging;

11° "haatpropagandisten": de natuurlijke personen of rechtspersonen, feitelijke verenigingen met inbegrip van alle de door hen aangewende middelen, ongeacht hun nationaliteit, verblijfplaats of plaats van vestiging, die voldoen aan volgende cumulatieve criteria:

a) zij hebben tot doel schade te berokkenen aan de beginselen van de democratie of de mensenrechten, de goede werking van de democratische instellingen of andere grondslagen van de rechtsstaat;

b) het gebruik van geweld of dwang als actiemethode rechtvaardigen;

c) deze overtuiging verspreiden naar anderen met de bedoeling om een radicaliserende invloed uit te oefenen; wordt verstaan onder "radicaliserende invloed": elke actie gepleegd door een entiteit met als doelstelling om een radicaliseringsproces overeenkomstig artikel 3, 15°, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten te initiëren, te ondersteunen of ertoe bij te dragen;

d) met een aanknopingspunt in België;

12° "persoonsgegevens": persoonsgegevens overeenkomstig artikel 4, 1), van de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen

physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) et de l'article 26, 1°, de la loi relative à la protection des données;

13° "informations": informations non classifiées conformément à la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité que les services de base et les services partenaires traitent dans le cadre de leurs missions légales respectives;

14° "banque de données commune T.E.R.": la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" visée à l'article 3;

15° "évaluation de la menace": évaluation, au sens de l'article 8, alinéa 1^{er}, 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace, pour les entités reprises dans la banque de données commune T.E.R.;

16° "fiche de renseignements": fiche qui contient l'ensemble des données à caractère personnel et des informations relatives à une entité de la banque de données commune T.E.R. provenant de l'ensemble des services qui l'alimentent;

17° "carte d'information": fiche d'une entité qui consiste en un extrait de la fiche de renseignements, contenant les données à caractère personnel et informations adéquates, pertinentes et non excessives au destinataire, pour le suivi des entités validées, pour le suivi des entités validées;

18° "droit de création": l'enregistrement d'une nouvelle entité dans la banque de données commune T.E.R.;

19° "droit de lecture": la consultation de l'ensemble des données à caractère personnel et des informations de la banque de données commune T.E.R.;

20° "droit d'écriture": l'introduction, modification ou effacement des données à caractère personnel et des informations dans la banque de données commune T.E.R.;

21° "droit d'interrogation": prise de connaissance de l'existence d'une entité dans la banque de données commune T.E.R. et en cas de confirmation de l'existence d'une entité dans la banque de données commune T.E.R., la prise de connaissance de l'évaluation de la menace;

22° "autorités de contrôle": l'Organe de contrôle de l'information policière, visé à l'article 71 de la loi relative à la protection des données et le Comité permanent de

in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening Gegevensbescherming) en artikel 26, 1° van de wet gegevensbescherming;

13° "informatie": niet-geclassificeerde informatie overeenkomstig de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen die de basisdiensten en de partnerdiensten verwerken in het kader van hun respectievelijke wettelijke opdrachten;

14° "gemeenschappelijke gegevensbank T.E.R.": de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" bedoeld in artikel 3;

15° "dreigingsevaluatie": evaluatie in de zin van artikel 8, eerste lid, 2°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging voor de entiteiten die zijn opgenomen in de gemeenschappelijke gegevensbank T.E.R.;

16° "inlichtingenfiche": fiche die alle persoonsgegevens en informatie met betrekking tot een entiteit van de gemeenschappelijke gegevensbank T.E.R. bevat die afkomstig zijn van alle diensten die haar voeden;

17° "informatiekaart": fiche van een entiteit die een uittreksel van de inlichtingenfiche vormt, en die de persoonsgegevens en informatie bevat die toereikend, ter zake dienend en niet overmatig zijn voor de bestemming, voor de opvolging van de gevalideerde entiteiten;

18° "creatierecht": de opname van een nieuwe entiteit in de gemeenschappelijke gegevensbank T.E.R.;

19° "leesrecht": de raadpleging van alle persoonsgegevens en informatie in de gemeenschappelijke gegevensbank T.E.R.;

20° "schrijfrecht": de invoering, wijziging of uitwissing van de persoonsgegevens en informatie in de gemeenschappelijke gegevensbank T.E.R.;

21° "vraagrecht": kennisneming van het bestaan van een entiteit in de gemeenschappelijke gegevensbank T.E.R. en, in geval van bevestiging van het bestaan van een entiteit in de gemeenschappelijke gegevensbank T.E.R., kennisneming van de dreigingsevaluatie;

22° "toezichthoudende overheden": het Controleorgaan op de politionele informatie, bedoeld in artikel 71 van de wet gegevensbescherming, en het Vast Comité van

contrôle des services de renseignement et de sécurité, visé à l'article 1^{er} de la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace;

23° "interconnexion": traitement, au moyen de procédés automatisés, par lequel

a) les données à caractère personnel et les informations de la banque de données commune T.E.R. sont mises en relation avec des données à caractère personnel et informations pertinentes enregistrées dans d'autres banques de données gérées par les services de base ou les services partenaires;

b) les données à caractère personnel et les informations pertinentes des banques de données, sources authentiques, peuvent être transférées vers la banque de données commune T.E.R.;

24° "délégué à la protection des données": le délégué à la protection des données visé à l'article 157/1 de la loi relative à la protection des données;

Section 1^{er}

Dispositions générales

Art. 3

Il est créé une banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" qui permet le traitement commun, par tout ou partie des services de base et des services partenaires, des données à caractère personnel et des informations relatives aux missions de prévention et de suivi du terrorisme et de l'extrémisme, lorsqu'il peut mener au terrorisme, au sens de l'article 8, 1°, b) et c), de la loi du 30 novembre 1998 des services de renseignement et de sécurité, de ces services, chacun dans le cadre de ses compétences légales.

La banque de données commune T.E.R. répond à la nécessité de structurer l'ensemble des données à caractère personnel et des informations relatives aux missions visées à l'alinéa premier fournies par les services de base et les services partenaires de sorte qu'elles soient retrouvées directement afin d'accomplir les finalités visées à l'article 5, alinéa 2.

Par dérogation à l'alinéa 2, les données à caractère personnel visées à l'article 6, paragraphe 2, 1°, point 1), b), ne peuvent pas être retrouvées directement.

Toezicht op de inlichtingen- en veiligheidsdiensten, bedoeld in artikel 1 van de organieke wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;

23° "koppeling": de verwerking, via geautomatiseerde procedures, waarbij

a) de persoonsgegevens en informatie van de gemeenschappelijke gegevensbank T.E.R. verbonden worden met persoonsgegevens en relevante informatie die geregistreerd zijn in andere gegevensbanken die door de basisdiensten of de partnerdiensten worden beheerd;

b) de persoonsgegevens en de relevante informatie van de gegevensbanken, authentieke bronnen, kunnen worden overgezonden aan de gemeenschappelijke gegevensbank T.E.R.;

24° "functionaris voor gegevensbescherming": de functionaris voor gegevensbescherming bedoeld in artikel 157/1 van de wet gegevensbescherming;

Afdeling 1

Algemene bepalingen

Art. 3

Er wordt een gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" gecreëerd die de gemeenschappelijke verwerking mogelijk maakt, door alle of een deel van de basisdiensten en de partnerdiensten, van de persoonsgegevens en informatie betreffende de opdrachten inzake de voorkoming en de opvolging van terrorisme en extremisme, dat kan leiden tot terrorisme, in de zin van artikel 8, 1°, b) en c), van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, van die diensten, elk in het kader van zijn wettelijke bevoegdheden.

De gemeenschappelijke gegevensbank T.E.R. beantwoordt aan de noodzaak tot het structureren van alle persoonsgegevens en informatie betreffende de opdrachten bedoeld in het eerste lid, die aangeleverd worden door de basisdiensten en de partnerdiensten, zodat zij direct worden teruggevonden teneinde de doeleinden bedoeld in artikel 5, tweede lid, te bereiken.

In afwijking van het tweede lid, mogen de in artikel 6, paragraaf 2, 1°, punt 1, onder b), bedoelde persoonsgegevens niet direct worden teruggevonden.

Une organisation dont l'objet réel est exclusivement d'ordre politique, syndical, philanthropique, philosophique ou religieux ou qui poursuit exclusivement tout autre but légitime ne peut, en tant que telle, être reprise dans la banque de données commune T.E.R.

Art. 4

Sans préjudice des articles 11 et 45 de la loi relative à la protection des données, les règles relatives à la protection des données et aux droits de la personne concernée sont celles visées au Titre 3, sous-titre 4, de la même loi.

Section 2

Responsables du traitement et finalités

Art. 5

Les ministres de l'Intérieur et de la Justice sont conjointement responsables du traitement de la banque de données commune T.E.R.

Les finalités de la banque de données commune T.E.R. sont les suivantes:

1° la concertation coordonnée entre les services de base et les services partenaires;

2° la nécessité stratégique, tactique ou opérationnelle de traiter en commun des données à caractère personnel et des informations pour exercer les missions respectives des services de base et des services partenaires;

3° l'aide à la prise de décisions par les autorités administratives ou à la prise de décisions de police administrative ou judiciaire;

4° l'analyse, l'évaluation et le suivi, en ce compris la prise de mesures, des entités validées enregistrées dans la banque de données commune T.E.R., l'analyse, l'évaluation et le suivi des entités en pré-enquêtes enregistrées dans la banque de données commune T.E.R. et l'analyse, l'évaluation et le suivi du phénomène du terrorisme et de l'extrémisme lorsqu'il peut mener au terrorisme;

5° l'aide à la protection, à l'accompagnement et au suivi des personnes suivantes:

Een organisatie waarvan het feitelijk oogmerk uitsluitend politiek, vakorganisatorisch, menslievend, levensbeschouwelijk of godsdienstig is of die uitsluitend enig ander rechtmatig oogmerk nastreeft, kan als zodanig niet in de gemeenschappelijke gegevensbank T.E.R. worden opgenomen.

Art. 4

Onverminderd artikelen 11 en 45 van de wet gegevensbescherming, zijn de regels inzake gegevensbescherming en inzake rechten van de betrokken persoon degene bedoeld in Titel 3, ondertitel 4, van dezelfde wet.

Afdeling 2

Verwerkingsverantwoordelijken en doeleinden

Art. 5

De ministers van Binnenlandse Zaken en van Justitie zijn gezamenlijk verantwoordelijk voor de verwerking van de gemeenschappelijke gegevensbank T.E.R.

De doeleinden van de gemeenschappelijke gegevensbank T.E.R. zijn de volgende:

1° het gecoördineerde overleg tussen de basisdiensten en de partnerdiensten;

2° de strategische, tactische of operationele noodzaak om gezamenlijk persoonsgegevens en informatie te verwerken voor het uitoefenen van de respectievelijke opdrachten van de basisdiensten en de partnerdiensten;

3° de hulp bij het nemen van beslissingen door de bestuurlijke overheden of bij het nemen van beslissingen van bestuurlijke of gerechtelijke politie;

4° de analyse, de evaluatie en de opvolging, daaronder begrepen het nemen van maatregelen, van de in de gemeenschappelijke gegevensbank T.E.R. geregistreerde gevalideerde entiteiten, de analyse, de evaluatie en de opvolging van de in de gemeenschappelijke gegevensbank T.E.R. geregistreerde entiteiten in vooronderzoek en de analyse, de evaluatie en de opvolging van het fenomeen van terrorisme en extremisme wanneer het kan leiden tot terrorisme;

5° de hulp bij de bescherming, de begeleiding en de opvolging van de volgende personen:

a) les mineurs de douze ans et plus qui sont considérés comme *foreign terrorist fighters*, *homegrown terrorist fighters*, extrémistes potentiellement violents, personnes condamnées pour terrorisme ou propagandistes de haine;

b) les enfants mineurs d'un *foreign terrorist fighter* qui répond aux critères visés à l'article 2, 7°, a) ou c), et qui ne sont pas ou ne peuvent pas être considérés comme *foreign terrorist fighters*, *homegrown terrorist fighters*, extrémistes potentiellement violents, personnes condamnées pour terrorisme ou propagandistes de haine.

Section 3

Traitement des données à caractère personnel

Art. 6

§ 1^{er}. La banque de données commune T.E.R. nécessite le traitement de différentes catégories de données à caractère personnel relatives aux personnes, aux groupements, aux organisations et aux phénomènes qui sont adéquates, pertinentes et non excessives au regard des missions visées à l'article 3, et des finalités visées à l'article 5, alinéa 2.

Les données à caractère personnel visées à l'alinéa 1^{er} présentent un lien direct avec la finalité du traitement.

§ 2. Les données à caractère personnel traitées dans la banque de données commune T.E.R. sont les données non classifiées au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité suivantes:

1° les données des entités suivantes:

1) Si l'entité est une personne physique majeure ou mineure de douze ans et plus:

a) les données d'identification suivantes:

i. nom, prénoms, alias;

ii. s'il échet, le numéro d'identification du Registre national des personnes physiques ou du registre des étrangers;

iii. l'adresse;

iv. le sexe et/ou le genre;

a) minderjarigen van twaalf jaar en ouder die worden beschouwd als *foreign terrorist fighters*, *homegrown terrorist fighters*, potentieel gewelddadige extremisten, terrorismeveroordeelden of haatpropagandisten;

b) de minderjarige kinderen van een *foreign terrorist fighter* die beantwoordt aan de criteria bedoeld in artikel 2, 7°, a) of c), die niet worden beschouwd of niet kunnen worden beschouwd als *foreign terrorist fighters*, *homegrown terrorist fighters*, potentieel gewelddadige extremisten, terrorismeveroordeelden of haatpropagandisten.

Afdeling 3

Verwerking van persoonsgegevens

Art. 6

§ 1. De gemeenschappelijke gegevensbank T.E.R. vereist de verwerking van verschillende categorieën van persoonsgegevens met betrekking tot personen, groeperingen, organisaties en fenomenen die toereikend, ter zake dienend en niet overmatig zijn in verhouding tot de opdrachten bedoeld in artikel 3, en de doeleinden bedoeld in artikel 5, tweede lid.

De persoonsgegevens bedoeld in het eerste lid staan in rechtstreeks verband met het doeleinde van de verwerking.

§ 2. De in de gemeenschappelijke gegevensbank T.E.R. verwerkte persoonsgegevens zijn de volgende in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen niet-geclassificeerde gegevens:

1° de gegevens van de volgende entiteiten:

1) Als de entiteit een meerderjarige natuurlijke persoon of een minderjarige natuurlijke persoon van twaalf jaar en ouder is:

a) de volgende identificatiegegevens:

i. naam, voornamen, alias;

ii. indien van toepassing, het identificatienummer van het Rijksregister van de natuurlijke personen of in het vreemdelingenregister;

iii. het adres;

iv. het geslacht en/of het gender;

v. la date, le lieu et le pays de naissance;	v. de geboortedatum, de geboorteplaats en het geboorteland;
vi. la ou les nationalité(s);	vi. de nationaliteit(en);
vii. la description physique;	vii. de fysieke beschrijving;
viii. des photos;	viii. foto's;
ix. s'il échet, la référence dactyloscopique unique;	ix. indien van toepassing, de unieke dactyloscopische referentie;
x. l'état civil;	x. de burgerlijke staat;
xi. la situation familiale;	xi. de gezinsituatie;
xii. la profession;	xii. het beroep;
xiii. les éléments liés à sa localisation;	xiii. de elementen in verband met de locatie;
xiv. les moyens de communication;	xiv. de communicatiemiddelen;
b) les données d'identification visées au point a), i. à v. des enfants mineurs visés à l'article 5, alinéa 2, 5°, b);	b) de onder a), i. tot v. bedoelde identificatiegegevens van de minderjarige kinderen bedoeld in artikel 5, tweede lid, 5°, b);
c) les données relatives aux catégories particulières de données à caractère personnel suivantes:	c) de volgende gegevens betreffende bijzondere categorieën van persoonsgegevens:
i. l'origine ethnique;	i. de etnische afkomst;
ii. les opinions politiques;	ii. de politieke opvattingen;
iii. les convictions religieuses ou philosophiques;	iii. de godsdienstige of levensbeschouwelijke overtuiging;
iv. les données biométriques aux fins d'identifier une personne physique de manière unique;	iv. de biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon;
v. les données concernant la santé;	v. de gegevens over de gezondheid;
d) les données relatives aux formations suivies;	d) de gegevens met betrekking tot gevolgde opleidingen;
e) les données relatives à la situation financière;	e) de gegevens met betrekking tot de financiële positie;
f) les données relatives aux fréquentations à risque;	f) de gegevens met betrekking tot risicovolle verplaatsingen;
g) les données relatives aux absences de réponse aux convocations de l'autorité;	g) de gegevens met betrekking tot het niet reageren op de oproepingen van de autoriteit;
h) les moyens de transports;	h) de vervoersmiddelen;
2) Si l'entité est une personne morale:	2) Als de entiteit een rechtspersoon is:

- a) la dénomination et s'il échet l'abréviation;
- b) le pays d'origine;
- c) l'adresse du siège;
- d) le type d'activités;
- e) les éléments liés à sa localisation;
- f) les moyens de transport;
- g) les moyens de communication;
- h) les personnes autorisées à l'administrer et à la représenter;

i) la situation juridique;

3) Si l'entité est une association de fait:

- a) la dénomination et s'il échet l'abréviation;
- b) le pays d'origine;
- c) l'adresse du siège;
- d) le type d'activités;
- e) les éléments liés à sa localisation;
- f) les moyens de transport;
- g) les moyens de communication;
- h) les personnes autorisées à l'administrer et à la représenter;

2° les données administratives, judiciaires, en ce compris celles sur les faits qualifiés d'infraction, de police judiciaire, de police administrative et les informations relatives aux entités enregistrées, traitées conformément à la loi par les services de base et les services partenaires qui disposent d'un droit de lecture et d'un droit d'écriture dans la banque de données commune T.E.R. et qui sont adéquates, pertinentes et non excessives au regard des missions visées à l'article 3 et des finalités visées à l'article 5, alinéa 2;

3° les données ou codes d'identification des personnes ou des services ayant accès à la banque de données commune T.E.R.

Les données visées à l'alinéa 1^{er}, 1°, point 1), c), v., sont traitées uniquement dans le but de comprendre le

- a) de naam en, indien van toepassing, de afkorting;
- b) het land van oorsprong;
- c) het adres van de zetel;
- d) de aard van de activiteiten;
- e) de elementen met betrekking tot de locatie;
- f) de vervoermiddelen;
- g) de communicatiemiddelen;
- h) de personen die bevoegd zijn om haar te beheren en te vertegenwoordigen;

i) de rechtstoestand;

3) Als de entiteit een feitelijke vereniging is:

- a) de naam en, indien van toepassing, de afkorting;
- b) het land van oorsprong;
- c) het adres van de zetel;
- d) de aard van de activiteiten;
- e) de elementen met betrekking tot de locatie;
- f) de vervoermiddelen;
- g) de communicatiemiddelen;
- h) de personen die bevoegd zijn om haar te beheren en te vertegenwoordigen;

2° de administratieve gegevens, de gerechtelijke gegevens, met inbegrip van de gegevens over strafbare feiten, de gegevens van gerechtelijke politie, de gegevens van bestuurlijke politie en de informatie betreffende de geregistreerde entiteiten, die overeenkomstig de wet verwerkt worden door de basisdiensten en de partnerdiensten die een leesrecht en een schrijfrecht hebben in de gemeenschappelijke gegevensbank T.E.R. en die toereikend, ter zake dienend en niet overmatig zijn in het licht van de opdrachten bedoeld in artikel 3 en de doeleinden bedoeld in artikel 5, tweede lid;

3° de identificatiegegevens of de identificatiecodes van de personen of de diensten die toegang hebben tot de gemeenschappelijke gegevensbank T.E.R.

De gegevens bedoeld in het eerste lid, 1°, punt 1), c, v., worden enkel verwerkt met het oog op het begrijpen

contexte médical somatique et mental lié à la personne concernée en lien direct avec les finalités visées à l'article 5, alinéa 2, ainsi que pour assurer la sécurité et protéger l'intégrité psychique et physique de toute personne susceptible d'entrer en contact avec les personnes concernées dans le cadre de l'intervention des autorités compétentes ou pour réaliser une évaluation de la menace. Lorsque des données relatives à la santé sont traitées, il est mentionné si ces données proviennent ou non de prestataires de soins.

Dans l'intérêt de la personne concernée et de celle d'un prestataire de soins, le service de base qui est en contact avec celui-ci lui communique, les données visées à l'alinéa 1^{er}, 1°, point 1), c), v. nécessaires enregistrées dans la banque de données commune T.E.R. et les données issues de l'évaluation de la menace relatives à la dangerosité de la personne concernée.

Le Roi détermine, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, les mesures nécessaires en vue d'assurer la gestion et la sécurité des données à caractère personnel et des informations traitées dans la banque de données commune T.E.R.

Art. 7

§ 1^{er}. Les données à caractère personnel conservées dans la banque de données commune T.E.R. sont archivées dès que les finalités visées à l'article 5, alinéa 2, ne sont plus rencontrées, et au maximum 30 ans après le dernier enregistrement d'une donnée ou information dans la fiche de renseignement de l'entité validée, à l'exception des données à caractère personnel relatives à des mineurs qui sont conservées au maximum 15 ans après le dernier enregistrement d'une donnée ou information.

Après le dernier enregistrement d'une donnée ou information dans la fiche de renseignement de l'entité validée, le responsable opérationnel examine tous les cinq ans si les données à caractère personnel présentent toujours un lien direct avec l'une des finalités de l'article 5, alinéa 2. Si tel n'est pas le cas, les données sont archivées.

Lorsque les données à caractère personnel sont relatives à des mineurs, l'examen visé à l'alinéa 2 a lieu tous les trois ans.

§ 2. Par dérogation au paragraphe 1^{er}, les données à caractère personnel et les informations relative à une

van de medische somatische en geestelijke omstandigheden waarin de betrokken persoon zich bevindt, in rechtstreeks verband met de in artikel 5, tweede lid, genoemde doeleinden, evenals om de veiligheid te garanderen en de psychische en fysieke integriteit te beschermen van elke persoon die in contact zou kunnen komen met de betrokken personen in het kader van de interventie door de bevoegde overheden ofwel om een dreigingsevaluatie op te stellen. Wanneer gezondheidsgegevens worden verwerkt, wordt vermeld of deze gegevens al dan niet afkomstig zijn van zorgverleners.

In het belang van de betrokken persoon en van een zorgverlener deelt de basisdienst die met laatstgenoemde in contact staat, hem de nodige gegevens bedoeld in het eerste lid, 1°, punt 1), c, v. mee die geregistreerd zijn in de gemeenschappelijke gegevensbank T.E.R. alsook de gegevens die afkomstig zijn van de dreigingsevaluatie met betrekking tot het gevaar dat uitgaat van de betrokken persoon.

De Koning bepaalt, bij een in Ministerraad overlegd besluit en na advies van de toezichthoudende overheden, de maatregelen die nodig zijn om het beheer en de veiligheid van de persoonsgegevens en de informatie die worden verwerkt in de gemeenschappelijke gegevensbank T.E.R. te verzekeren.

Art. 7

§ 1. De in de gemeenschappelijke gegevensbank T.E.R. bewaarde persoonsgegevens worden gearchiveerd vanaf het ogenblik dat de doeleinden bedoeld in artikel 5, tweede lid, niet meer worden bereikt, en ten laatste 30 jaar na de laatste opname van een gegeven of van informatie in de inlichtingenfiche van de gevalideerde entiteit, met uitzondering van de persoonsgegevens van minderjarigen, die tot maximaal 15 jaar na de laatste opname van een gegeven of van informatie worden bewaard.

Na de laatste opname van een gegeven of van informatie in de inlichtingenfiche van de gevalideerde entiteit onderzoekt de operationeel verantwoordelijke om de vijf jaar of de persoonsgegevens nog steeds een rechtstreeks verband vertonen met een van de doeleinden van artikel 5, tweede lid. Indien dit niet het geval is, worden de gegevens gearchiveerd.

Wanneer de persoonsgegevens betrekking hebben op minderjarigen, vindt het in het tweede lid bedoelde onderzoek om de drie jaar plaats.

§ 2. In afwijking van paragraaf 1, worden de persoonsgegevens en informatie met betrekking tot een entiteit

entité en pré-enquêtes sont conservées pour une durée de maximum six mois après leur enregistrement.

À l'issue de ce délai, les données à caractère personnel et les informations sont supprimées de la banque de données commune T.E.R. conformément au paragraphe 3, alinéa 2, dès lors que l'entité en pré-enquête ne répond pas aux critères d'un *foreign terrorist fighter*, *homegrown terrorist fighter*, extrémiste potentiellement violent ou d'un propagandiste de haine.

§ 3. Les données à caractère personnel et les informations qui doivent être archivées le sont pour une durée de maximum 30 ans.

À l'issue de ce délai, ces données et informations sont supprimées de la banque de données commune T.E.R., sans préjudice de la loi du 24 juin 1955 relative aux archives.

Lorsqu'une donnée ou information relative à une entité enregistrée se révèle être fausse ou erronée, elle est immédiatement supprimée.

La consultation des archives de la banque de données commune T.E.R. ne peut être réalisée que dans le cadre des finalités suivantes:

1° l'appui à la définition et à la réalisation de la politique de sécurité en matière de terrorisme et d'extrémisme pouvant mener au terrorisme;

2° le traitement des antécédents dans le cadre d'une enquête judiciaire ou de renseignement relative au terrorisme ou à l'extrémisme pouvant mener au terrorisme;

3° la défense en justice des autorités visées à l'article 5, alinéa 2, 3°;

4° l'exercice des missions des autorités de contrôle;

5° la réalisation de finalités historiques, scientifiques ou statistiques.

Le résultat de l'exploitation des archives de la banque de données commune T.E.R. pour la finalité prévue à l'alinéa 4, 1°, est anonymisé.

§ 4. Si dans le cadre de la consultation visée au paragraphe 3, alinéa 4, 2°, les données archivées répondent de nouveau à la finalité visée à l'article 5, alinéa 2, 2°, les données sont désarchivées.

in vooronderzoek, maximale zes maanden bewaard, te rekenen vanaf hun registratie.

Na afloop van deze termijn worden de persoonsgegevens en informatie verwijderd uit de gemeenschappelijke gegevensbank T.E.R. overeenkomstig paragraaf 3, tweede lid, wanneer de entiteit in vooronderzoek niet voldoet aan de criteria van een *foreign terrorist fighter*, *homegrown terrorist fighter*, potentieel gewelddadige extremist of haatpropagandist.

§ 3. De persoonsgegevens en de informatie die moeten worden gearcheeerd, worden gearcheeerd gedurende een termijn van maximaal 30 jaar.

Na afloop van deze termijn, worden deze gegevens en informatie verwijderd uit de gemeenschappelijke gegevensbank T.E.R. onverminderd de archiefwet van 24 juni 1955.

Wanneer een gegeven of informatie met betrekking tot een opgenomen entiteit fout of verkeerd blijkt te zijn, wordt dat gegeven of die informatie onmiddellijk verwijderd.

De raadpleging van de archieven van de gemeenschappelijke gegevensbank T.E.R. mag slechts gebeuren in het kader van de volgende doeleinden:

1° de ondersteuning bij het bepalen en het uitwerken van veiligheidsbeleid inzake terrorisme en extremisme dat tot terrorisme kan leiden;

2° de verwerking van de antecedenen in het kader van een gerechtelijk onderzoek of inlichtingenonderzoek met betrekking tot een terrorisme of extremisme dat tot terrorisme kan leiden;

3° de verdediging in rechte van de overheden bedoeld in artikel 5, tweede lid, 3°;

4° de uitoefening van de opdrachten van de toezichthoudende autoriteiten;

5° de verwezenlijking van historische, wetenschappelijke of statistische doeleinden.

Het resultaat van de exploitatie van de archieven van de gemeenschappelijke gegevensbank T.E.R. voor het in het vierde lid, 1°, bedoelde doeleinde wordt geanonimiseerd.

§ 4. Als in het kader van de in paragraaf 3, vierde lid, 2°, bedoelde raadpleging de gearcheeerde gegevens opnieuw beantwoorden aan het in artikel 5, tweede lid, 2°, bedoelde doeleinde, worden de gegevens gedearchiveerd.

Art. 8

§ 1^{er}. Des fichiers de journalisation sont établis dans la banque de données commune T.E.R. pour les traitements suivants: la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction de données.

Les fichiers de journalisation de consultation et de communication permettent d'établir:

1° le motif, la date et l'heure de ces traitements;

2° les catégories de personnes qui ont consulté les données à caractère personnel, ainsi que l'identification ou le code d'identification de la personne ou du service qui a consulté ces données;

3° les systèmes qui ont communiqué ces données;

4° les catégories de destinataires des données à caractère personnel, et si possible, l'identité des destinataires de ces données.

L'ensemble des traitements des données figurant dans la banque de données commune T.E.R. font l'objet d'une journalisation qui est conservée pendant 30 ans à partir du moment de leur réalisation.

§ 2. En concertation avec le gestionnaire visé à l'article 11, le responsable opérationnel adopte des mesures appropriées pour assurer la sécurité des fichiers de journalisation et, en particulier, pour empêcher tout traitement non autorisé et pour assurer l'intégrité des données traitées.

§ 3. En concertation avec le gestionnaire visé à l'article 11, le responsable opérationnel adopte des procédures d'accès aux fichiers de journalisation, qui garantissent la nécessité et la proportionnalité de l'accès aux données de journalisation en vue d'atteindre les finalités de contrôle conformément à la loi relative à la protection des données.

§ 4. Le gestionnaire visé à l'article 11 veille à la bonne exécution des dispositions visées aux paragraphes 1 à 3.

Art. 8

§ 1. Logbestanden worden aangemaakt in de gemeenschappelijke gegevensbank T.E.R. voor de volgende verwerkingen: het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

De logbestanden van de raadpleging en de mededeling laten toe om:

1° de beweegreden, de datum en het tijdstip van die verwerkingen vast te stellen;

2° de categorieën van personen die de persoonsgegevens hebben geraadpleegd vast te stellen, alsook de identificatie of de identificatiecode van de persoon of de dienst die deze gegevens heeft geraadpleegd;

3° vast te stellen welke systemen die gegevens hebben meegedeeld;

4° de categorieën van ontvangers van de persoonsgegevens vast te stellen en indien mogelijk de identiteit van de ontvangers van die gegevens.

Alle verwerkingen van de gegevens die in de gemeenschappelijke gegevensbank T.E.R. staan, zijn het voorwerp van een logging die 30 jaar wordt bijgehouden vanaf de uitvoering ervan.

§ 2. In overleg met de in artikel 11 bedoelde beheerder neemt de operationeel verantwoordelijke gepaste maatregelen om de veiligheid van de logbestanden te verzekeren en, in het bijzonder om elke niet-toegelaten verwerking te beletten en de integriteit van de verwerkte gegevens te verzekeren.

§ 3. In overleg met de in artikel 11 bedoelde beheerder stelt de operationeel verantwoordelijke procedures voor toegang tot de logbestanden vast die waarborgen dat de toegang tot de logginggegevens noodzakelijk en evenredig is met het oog op het bereiken van de doeleinden inzake toezicht overeenkomstig de wet gegevensbescherming.

§ 4. De in artikel 11 bedoelde beheerder ziet toe op de goede uitvoering van de bepalingen bedoeld in paragrafen 1 tot 3.

Art. 9

§ 1^{er}. Dans le cadre des missions visées à l'article 3 et des finalités visées à l'article 5, alinéa 2, une interconnexion des données visées à l'article 6, paragraphe 2, alinéa 1^{er} et des informations enregistrées dans la banque de données commune T.E.R. peut être établie entre la banque de données commune T.E.R. et d'autres banques de données gérées par les services de base ou les services partenaires dans le cadre de leurs missions légales ou les sources authentiques de données visées au paragraphe 2.

Le Roi détermine, après avis des responsables du traitement des banques de données visées à l'alinéa 1^{er} et des autorités de contrôle compétentes, et pour les banques de données gérées par le partenaire visé à l'article 2, 3°, e), après accord du Collège du ministère public, les traitements visés par l'interconnexion, les catégories de données à caractère personnel interconnectées et les modalités d'interconnexion, lesquelles doivent respecter l'intégrité des données et des réseaux, en particulier pour ce qui concerne les banques de données qui contiennent des données classifiées au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

§ 2. Dans le cadre des missions visées à l'article 3 et des finalités visées à l'article 5, alinéa 2, pour les données visées à l'article 6, paragraphe 2, alinéa 1^{er}, 1°, point 1), a), i. à xii., une interconnexion peut être établie du Registre national des personnes physiques visé à l'article 1^{er} de la loi du 8 août 1983 organisant un Registre national des personnes physique vers la banque de données commune T.E.R.

Dans le cadre des missions visées à l'article 3 et des finalités visées à l'article 5, alinéa 2, pour les données visées à l'article 6, paragraphe 2, alinéa 1^{er}, 1°, point 2), a) à d), h) et i) et point 3), a) à d), h) et i), une interconnexion peut être établie de la Banque Carrefour des Entreprises visé à l'article III.15 du Code de droit économique vers la banque de données commune T.E.R.

Dans le cadre des missions visées à l'article 3 et des finalités visées à l'article 5, alinéa 2, pour les données visées à l'article 6, paragraphe 2, alinéa 1^{er}, 1°, point 1), h), point 2), f) et point 3), f), une interconnexion peut être établie du répertoire-matricule des véhicules visé à l'article 6 de l'arrêté royal du 20 juillet 2001 relatif à

Art. 9

§ 1. In het kader van de in artikel 3 bedoelde opdrachten en van de in artikel 5, tweede lid bedoelde doeleinden, kan een koppeling van de in artikel 6, paragraaf 2, eerste lid, bedoelde gegevens en de in de gemeenschappelijke gegevensbank T.E.R. opgenomen informatie tot stand worden gebracht tussen de gemeenschappelijke gegevensbank T.E.R. en andere gegevensbanken die worden beheerd door de basisdiensten of de partnerdiensten in het kader van hun wettelijke opdrachten of de authentieke gegevensbronnen als bedoeld in paragraaf 2.

De Koning bepaalt, na advies van de verwerkingsverantwoordelijken van de in het eerste lid bedoeld gegevensbanken en van de bevoegde toezichhoudende overheden, en voor wat de gegevensbanken beheerd door de partner bedoeld in artikel 2, 3°, e), betreft, na akkoord van het College van het openbaar ministerie, de verwerkingen die onder de koppeling vallen, de onderling verbonden categorieën van persoonsgegevens en de nadere regels van de koppeling, waarbij de integriteit van de gegevens en van de netwerken gerespecteerd moeten worden, in het bijzonder wat betreft de gegevensbanken die geclassificeerde gegevens bevatten in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

§ 2. In het kader van de in artikel 3 bedoelde opdrachten en de in artikel 5, tweede lid, bedoelde doeleinden, kan voor de gegevens bedoeld in artikel 6, paragraaf 2, eerste lid, 1°, punt 1) a), i. tot xii., een koppeling tot stand worden gebracht van het Rijksregister van de natuurlijke personen bedoeld in artikel 1 van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, naar de gemeenschappelijke gegevensbank T.E.R.

In het kader van de in artikel 3 bedoelde opdrachten en de in artikel 5, tweede lid, bedoelde doeleinden, kan voor de gegevens bedoeld in artikel 6, paragraaf 2, eerste lid, 1°, punt 2), a) tot d), h) en i) en punt 3), a) tot d), h) en i), een koppeling tot stand worden gebracht van de Kruispuntbank van Ondernemingen bedoeld in artikel III.15 van het Wetboek van economisch recht, naar de gemeenschappelijke gegevensbank T.E.R.

In het kader van de in artikel 3 bedoelde opdrachten en de in artikel 5, tweede lid, bedoelde doeleinden, kan voor de gegevens bedoeld in artikel 6, paragraaf 2, eerste lid, 1°, punt 1), h), punt 2), f) en punt 3), f), een koppeling tot stand worden gebracht van het repertorium van de voertuigen bedoeld in artikel 6 van het koninklijk

l'immatriculation de véhicules vers la banque de données commune T.E.R.

Dans le cadre des missions visées à l'article 3 et des finalités visées à l'article 5, alinéa 2, pour les personnes physiques et les personnes morales enregistrées dans la banque de données commune T.E.R., une interconnexion peut être établie du Casier judiciaire central visé à l'article 589 du Code d'instruction criminelle vers la banque de données commune T.E.R.

Art. 10

Le Roi peut, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, déterminer des modalités complémentaires de gestion de la banque de données commune T.E.R.

Section 4

Gestionnaire et responsable opérationnel

Art. 11

Sur proposition conjointe des ministres de l'Intérieur et de la Justice, le Roi désigne un gestionnaire chargé de la gestion technique et fonctionnelle de la banque de données commune T.E.R.

Le gestionnaire assure au moins les missions suivantes:

1° créer et mettre à la disposition la banque de données commune T.E.R. en recourant aux moyens techniques nécessaires sur la base des possibilités découlant de l'environnement ICT propre à son service;

2° gérer la banque de données commune T.E.R. et en assurer sa maintenance;

3° traduire en règles fonctionnelles les modalités relatives au traitement de l'information;

4° déterminer les normes techniques nécessaires au fonctionnement de la banque de données commune T.E.R. et les faire appliquer;

5° fournir un avis sur le plan technique et/ou fonctionnel à la demande du responsable opérationnel ou du délégué à la protection des données;

besluit van 20 juli 2001 betreffende de inschrijving van voertuigen, naar de gemeenschappelijke gegevensbank T.E.R.

In het kader van de in artikel 3 bedoelde opdrachten en de in artikel 5, tweede lid, bedoelde doeleinden kan, voor natuurlijke personen en rechtspersonen die in de gemeenschappelijke gegevens T.E.R. zijn geregistreerd, een koppeling tot stand worden gebracht van het Centraal Strafregister bedoeld in artikel 589 van het Wetboek van Strafvordering, naar de gemeenschappelijke gegevensbank T.E.R.

Art. 10

De Koning kan, bij een in Ministerraad overlegd besluit en na advies van de toezichthoudende overheden, bijkomende nadere beheersregels van de gemeenschappelijke gegevensbank T.E.R. bepalen.

Afdeling 4

Beheerder en operationeel verantwoordelijke

Art. 11

Op gezamenlijk voorstel van de ministers van Binnenlandse Zaken en van Justitie, wijst de Koning een beheerder aan die belast is met het technisch en functioneel beheer van de gemeenschappelijke gegevensbank T.E.R.

De beheerder verzekert minstens de volgende opdrachten:

1° het creëren en het ter beschikking stellen van de gemeenschappelijke gegevensbank T.E.R. door een beroep te doen op de noodzakelijke technische middelen op basis van de mogelijkheden die voortvloeien uit de ICT-omgeving eigen aan zijn dienst;

2° het beheren van de gemeenschappelijke gegevensbank T.E.R. en er het onderhoud van verzekeren;

3° de nadere regels met betrekking tot de verwerking van de informatie in functionele regels omzetten;

4° de technische normen bepalen die noodzakelijk zijn voor de werking van de gemeenschappelijke gegevensbank T.E.R. en deze doen toepassen;

5° een advies op technisch en/of functioneel vlak verstrekken op vraag van de operationeel verantwoordelijke of van de functionaris voor gegevensbescherming;

6° organiser les droits et les accès nécessaires aux traitements à effectuer dans la banque de données commune T.E.R.;

7° tenir la liste des personnes ou codes d'identification des personnes ou des services ayant accès à la banque de données commune T.E.R.;

8° veiller à la journalisation des traitements réalisés dans la banque de données commune T.E.R.;

9° fournir une documentation et une assistance technique.

Art. 12

Sur proposition conjointe des ministres de l'Intérieur et de la Justice, le Roi désigne un responsable opérationnel chargé de la gestion opérationnelle de la banque de données commune T.E.R.

Le responsable opérationnel assure au moins les missions suivantes:

1° contrôler la qualité des données traitées au sein de la banque de données commune T.E.R. et s'assurer de leur pertinence au regard des finalités pour lesquelles la banque de données a été créée;

2° exercer une fonction de coordination pour l'alimentation de la banque de données commune T.E.R. par les différents services;

3° organiser la collaboration adéquate entre le gestionnaire, les services de base et les services partenaires en vue de réaliser les finalités prévues;

4° veiller à ce que l'exploitation des données à caractère personnel et des informations réponde aux finalités décrites à l'article 5, alinéa 2;

5° valider l'enregistrement d'une personne physique majeure ou mineure de douze ans et plus, d'une personne morale ou une association de fait ainsi que de l'ensemble des moyens utilisés par celles-ci, dès lors qu'elle répond aux critères d'un *foreign terrorist fighter*, *homegrown terrorist fighter*, extrémiste potentiellement violent, d'une personne condamnée pour terrorisme ou d'un propagandiste de haine, dans la banque de données commune T.E.R. sur base de données et informations

6° de rechten en de toegangen organiseren die nodig zijn voor de te verrichte verwerkingen in de gemeenschappelijke gegevensbank T.E.R.;

7° het bijhouden van de lijst van de personen of de identificatiecodes van de personen of de diensten die over een toegang tot de gemeenschappelijke gegevensbank T.E.R. beschikken;

8° het waken over de logbestanden van de in de gemeenschappelijke gegevensbank T.E.R. uitgevoerde verwerkingen;

9° een documentatie en een technische ondersteuning aanbieden.

Art. 12

Op gezamenlijk voorstel van de ministers van Binnenlandse Zaken en van Justitie, wijst de Koning een operationeel verantwoordelijke aan die belast is met het operationeel beheer van de gemeenschappelijke gegevensbank T.E.R.

De operationeel verantwoordelijke verzekert minstens de volgende opdrachten:

1° het controleren van de kwaliteit van de in de gemeenschappelijke gegevensbank T.E.R. verwerkte gegevens en het zich verzekeren van de relevantie ervan in verhouding tot de doeleinden waarvoor de gegevensbank opgericht werd;

2° het uitoefenen van een coördinatiefunctie voor de voeding van de gemeenschappelijke gegevensbank T.E.R. door de verschillende diensten;

3° het organiseren van de passende samenwerking tussen de beheerder, de basisdiensten en de partnerdiensten met het oog op de verwezenlijking van de voorziene doeleinden;

4° erop toezien dat de exploitatie van de persoonsgegevens en de informatie beantwoordt aan de in artikel 5, tweede lid, beschreven doeleinden;

5° het valideren van de opname van een meerderjarige natuurlijke persoon of minderjarige natuurlijke persoon van twaalf jaar en ouder, van een rechtspersoon of feitelijke vereniging, alsook van alle de door hen aangewende middelen, indien zij beantwoordt aan de criteria van een *foreign terrorist fighter*, *homegrown terrorist fighter*, potentieel gewelddadige extremist, terrorismeveroordeelde of haatpropagandist in de gemeenschappelijke gegevensbank T.E.R. op basis van

qui y sont introduites, selon les modalités déterminées par le Roi;

6° informer le service qui alimente la banque de données commune T.E.R. lorsque le responsable opérationnel évalue que la donnée transmise ne remplit pas ou plus un caractère adéquat, pertinent et non excessif au regard des missions visées à l'article 3, et des finalités visées à l'article 5, alinéa 2, et conclut que celle-ci doit dès lors être supprimée de la banque de données commune.

Art. 13

§ 1^{er}. Le responsable opérationnel gère et traite les brèches de sécurité de la banque de données commune T.E.R. constatées personnellement ou rapportées conformément aux paragraphes 2 et 3. Pour l'application du présent article, on entend par "brèche de sécurité", toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Les brèches de sécurité de nature technique et fonctionnelle sont gérées par le gestionnaire en collaboration avec le responsable opérationnel.

§ 2. Le responsable opérationnel informe dans les plus brefs délais le gestionnaire et le délégué à la protection des données, de toute brèche de sécurité.

Le responsable opérationnel est le point de contact pour le responsable du traitement visé à l'article 5, alinéa 1^{er}, et l'informe des éventuelles brèches de sécurité.

En cas de brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable opérationnel la notifie aux autorités de contrôle dans les meilleurs délais.

§ 3. La notification visée au paragraphe 2, alinéa 3, décrit ou communique, à tout le moins:

1° la nature de la brèche de sécurité y compris, si possible, le nombre estimé de personnes et d'enregistrements de données à caractère personnel concernés;

gegevens en informatie die daarin worden ingevoerd, op de wijze bepaald door de Koning;

6° het in kennis stellen van de dienst die de gemeenschappelijke gegevensbank T.E.R. voedt wanneer de operationeel verantwoordelijke oordeelt dat het doorgezonden gegeven niet of niet langer toereikend, ter zake dienend en niet-overmatig is in het licht van de opdrachten bedoeld in artikel 3 en ten opzichte van de doeleinden beoogd in artikel 5, tweede lid, en hij besluit dat dit gegeven daarom verwijderd moet worden uit de gemeenschappelijke gegevensbank.

Art. 13

§ 1. De operationeel verantwoordelijke beheert en behandelt de inbreuken op de beveiliging van de gemeenschappelijke gegevensbank T.E.R. die persoonlijk worden vastgesteld of die overeenkomstig paragrafen 2 en 3 worden gerapporteerd. Voor de toepassing van dit artikel, wordt verstaan onder "inbreuk op de beveiliging", elke inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde bekendmaking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Inbreuken op de beveiliging van technische en functionele aard worden beheerd door de beheerder in samenwerking met de operationeel verantwoordelijke.

§ 2. De operationeel verantwoordelijke stelt de beheerder en de functionaris voor gegevensbescherming zo snel mogelijk in kennis van elke inbreuk op de beveiliging.

De operationeel verantwoordelijke is het contactpunt voor de verwerkingsverantwoordelijke bedoeld in artikel 5, eerste lid, en stelt hem in kennis van eventuele inbreuken op de beveiliging.

In geval van een inbreuk op de beveiliging die aanleiding kan vormen tot een hoog risico voor de rechten en vrijheden van natuurlijke personen, meldt de operationeel verantwoordelijke deze inbreuk zo snel mogelijk aan de toezichthoudende overheden.

§ 3. In de in paragraaf 2, derde lid bedoelde melding wordt, op zijn minst, het volgende omschreven of meegedeeld:

1° de aard van de inbreuk op de beveiliging, en indien mogelijk, bij benadering, het aantal betrokkenen en de opgeslagen persoonsgegevens in kwestie;

2° le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

3° les conséquences probables de la brèche de sécurité;

4° les mesures que le responsable opérationnel a prises ou propose de prendre pour remédier à la brèche de sécurité, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Section 5

Droits d'accès dans la banque de données commune T.E.R.

Art. 14

Sur la base du respect des principes d'adéquation, de pertinence et du caractère non excessif, dans le cadre de l'exercice de leurs missions visées à l'article 3, et conformément aux finalités de l'article 5, alinéa 2, chacun dans le cadre de ses compétences respectives, les services de base disposent d'un droit de création, d'un droit de lecture et d'un droit d'écriture dans la banque de données commune T.E.R.

Art. 15

§ 1^{er}. Dans le cadre de l'exercice de leurs missions, les autorités de contrôle disposent d'un droit de lecture dans la banque de données commune T.E.R.

§ 2. Dans le cadre de l'exercice de leurs missions, le Comité permanent de contrôle des services de police et son service enquêtes disposent d'un droit de lecture dans la banque de données commune T.E.R.

§ 3. Dans le cadre de l'exercice de ses missions, l'Inspection générale de la police fédérale et de la police locale dispose d'un droit de lecture dans la banque de données commune T.E.R.

Art. 16

Sur la base du respect des principes d'adéquation, de pertinence et du caractère non excessif, dans le cadre de l'exercice de leurs missions visées à l'article 3, et conformément aux finalités de l'article 5, alinéa 2,

2° de la naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar bijkomende informatie kan worden verkregen;

3° de waarschijnlijke gevolgen van de inbreuk op de beveiliging;

4° de maatregelen die de operationeel verantwoordelijke heeft voorgesteld of genomen om de inbreuk op de beveiliging aan te pakken, waaronder desgevallend maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Afdeling 5

Toegangsrechten in de gemeenschappelijke gegevensbank T.E.R.

Art. 14

Op basis van de inachtneming van de principes van toereikendheid, relevantie en de niet-bovenmatige aard in het kader van de uitoefening van hun opdrachten bedoeld in artikel 3 en overeenkomstig de doeleinden van artikel 5, tweede lid, beschikken de basisdiensten, elk in het kader van hun respectieve bevoegdheden, over een creatierecht, een leesrecht en een schrijfrecht in de gemeenschappelijke gegevensbank T.E.R.

Art. 15

§ 1. In het kader van de uitoefening van hun opdrachten beschikken de toezichthoudende overheden over een leesrecht in de gemeenschappelijke gegevensbank T.E.R.

§ 2. In het kader van de uitoefening van hun opdrachten, beschikken het Vast Comité van Toezicht op de politiediensten en zijn Dienst Enquêtes over een leesrecht in de gemeenschappelijke gegevensbank T.E.R.

§ 3. In het kader van de uitoefening van hun opdrachten, beschikt de Algemene Inspectie van de Federale Politie en van de Lokale Politie over een leesrecht in de gemeenschappelijke gegevensbank T.E.R.

Art. 16

Op basis van de inachtneming van de principes van toereikendheid, relevantie en de niet-bovenmatige aard in het kader van de uitoefening van hun opdrachten bedoeld in artikel 3 en overeenkomstig de doeleinden

chacun dans le cadre de ses compétences respectives, les services partenaires peuvent disposer:

1° d'un droit de lecture et d'un droit d'écriture dans la banque de données commune T.E.R.; ou

2° d'un droit d'interrogation dans la banque de données commune T.E.R.

Le Roi détermine, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, pour chaque service partenaire, le type de droit et ses modalités d'exercice.

Pour le service partenaire visé à l'article 2, 3°, e), le Roi détermine, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle et avis conforme du Collège des procureurs généraux, le type de droit et ses modalités d'exercice.

Section 6

Création d'une entité et alimentation de la banque de données commune T.E.R.

Art. 17

Seul un service de base dispose d'un droit de création dans la banque de données commune T.E.R.

Art. 18

Les services de base et les services partenaires qui bénéficient d'un droit de lecture et d'un droit d'écriture sont tenus respectivement de consulter la banque de données commune T.E.R. et d'y introduire d'office leurs propres données à caractère personnel et les informations pertinentes. Ces données à caractère personnel et informations sont enregistrées dans la banque de données commune T.E.R., sous leur responsabilité et suivant leurs procédures internes de validation.

Les données à caractère personnel et informations enregistrées dans la banque de données commune T.E.R. en application de l'alinéa 1^{er} proviennent des données à caractère personnel et informations qui sont à disposition des services de base et des services partenaires dans le cadre de leurs missions respectives et des finalités qui y sont liées.

van artikel 5, tweede lid, kunnen de partnerdiensten, elk in het kader van hun respectieve bevoegdheden, beschikken over:

1° een leesrecht en een schrijfrecht in de gemeenschappelijke gegevensbank T.E.R.; of

2° een vraagrecht in de gemeenschappelijke gegevensbank T.E.R.

De Koning bepaalt, bij een in Ministerraad overlegd besluit en na advies van de toezichhoudende overheden, voor iedere partnerdienst de aard van het recht en de nadere regels van de uitoefening ervan.

Voor de partnerdienst bedoeld in artikel 2, 3°, e), bepaalt de Koning, bij een in Ministerraad overlegd besluit en na advies van de toezichhoudende overheden en na eensluidend advies van het College van procureurs-generaal, de aard van het recht en de nadere regels van de uitoefening ervan.

Afdeling 6

Creatie van een entiteit en voeding van de gemeenschappelijke gegevensbank T.E.R.

Art. 17

Alleen een basisdienst beschikt over een creatierecht in de gemeenschappelijke gegevensbank T.E.R.

Art. 18

De basisdiensten en de partnerdiensten die een leesrecht en een schrijfrecht hebben zijn verplicht respectievelijk de gemeenschappelijke gegevensbank T.E.R. te raadplegen en ambtshalve hun eigen persoonsgegevens en relevante informatie daarin in te voeren. Die persoonsgegevens en informatie worden onder hun verantwoordelijkheid en overeenkomstig hun interne validatieprocedures opgenomen in de gemeenschappelijke gegevensbank T.E.R.

De persoonsgegevens en informatie die overeenkomstig het eerste lid in de gemeenschappelijke gegevensbank T.E.R. worden opgenomen, worden afgeleid uit de persoonsgegevens en informatie waarover de basisdiensten en de partnerdiensten beschikken in het kader van hun respectieve opdrachten en de daarmee verband houdende doeleinden.

L'article 458 du Code pénal ne peut être invoqué lorsque les services de base ou les services partenaires exercent leur droit d'écriture dans la banque de données commune T.E.R. conformément à la présente section.

Les services de police saisissent les données à caractère personnel et les informations visées à l'alinéa 1^{er}, conformément aux spécifications supplémentaires énoncées dans une directive du Collège des procureurs généraux visant à sauvegarder le secret de l'instruction tel que prévu aux articles 28quinquies et 57 du Code d'instruction criminelle et l'exercice de l'action publique.

Art. 19

Par dérogation à l'article 17 et à l'article 18, alinéa 1^{er}, le droit de création et le droit d'écriture dans la banque de données commune T.E.R. sont différés lorsque et aussi longtemps que le magistrat compétent, avec l'accord du procureur fédéral, estime que cette création et cette alimentation peuvent compromettre l'exercice de l'action publique, la sécurité d'une personne ou la relation avec un service répressif d'un État étranger. Le cas échéant, le procureur fédéral peut déterminer les modalités de cette dérogation. Le procureur fédéral vérifie, à échéances régulières, la nécessité du maintien de l'ajournement de la création et de l'alimentation de la banque de données commune T.E.R.

Par dérogation à l'article 17 et à l'article 18, alinéa 1^{er}, le droit de création et le droit d'écriture dans la banque de données commune T.E.R. sont différés, lorsque et aussi longtemps que le dirigeant d'un service du renseignement et de sécurité estime que cette création et cette alimentation peuvent compromettre la sécurité d'une personne, l'exercice d'une enquête de renseignement ou la relation avec un service de renseignement et de sécurité d'un État étranger.

Section 7

*Communication des données
à caractère personnel et des informations*

Art. 20

La fiche de renseignements est uniquement accessible aux services qui ont un droit de lecture et un droit d'écriture dans la banque de données commune T.E.R. et ne peut pas être communiquée à d'autres services

Artikel 458 van het Strafwetboek kan niet ingeroepen worden wanneer een basisdienst of een partnerdienst in het kader van de bepalingen in deze afdeling haar schrijfrecht uitoefent in de gemeenschappelijke gegevensbank T.E.R.

De politiediensten voeren de persoonsgegevens en informatie bedoeld in het eerste lid in overeenkomstig de aanvullende specificaties vastgesteld in een richtlijn van het College van procureurs-generaal strekkende tot de vrijwaring van het geheim van het onderzoek zoals bedoeld in de artikelen 28quinquies en 57 van het Wetboek van Strafvordering en van de uitoefening van de strafvordering.

Art. 19

In afwijking van artikel 17 en artikel 18, eerste lid, worden het creatierecht en het schrijfrecht in de gemeenschappelijke gegevensbank T.E.R. uitgesteld wanneer en zolang de bevoegde magistraat, met toestemming van de federale procureur, meent dat deze creatie en deze voeding de uitoefening van de strafvordering, de veiligheid van een persoon of de relatie met een rechtshandavingsinstantie van een buitenlandse Staat in het gedrang kunnen brengen. In voorkomend geval kan de federale procureur de nadere regels voor deze afwijking bepalen. De federale procureur gaat op regelmatige tijdstippen de noodzaak tot behoud van het uitstel van de creatie en de voeding van de gemeenschappelijke gegevensbank T.E.R. na.

In afwijking van artikel 17 en artikel 18, eerste lid, worden het creatierecht en het schrijfrecht in de gemeenschappelijke gegevensbank T.E.R. uitgesteld wanneer en zolang de leidinggevende van een inlichtingen- en veiligheidsdienst meent dat deze creatie en deze voeding de veiligheid van een persoon, de uitoefening van een inlichtingenonderzoek of de relatie met een inlichtingen- en veiligheidsdienst van een buitenlandse Staat in het gedrang kunnen brengen.

Afdeling 7

*Mededeling
van de persoonsgegevens en de informatie*

Art. 20

De inlichtingenfiche is enkel toegankelijk voor de diensten die een leesrecht en een schrijfrecht in de gemeenschappelijke gegevensbank T.E.R. hebben, en mag niet worden meegedeeld aan andere diensten of

ou institutions à l'exception des autorités de contrôle dans le cadre de leurs missions.

Art. 21

La création d'une nouvelle entité dans la banque de données commune T.E.R. est immédiatement communiquée au président de la Task force locale visée à l'article 31 et au chef de corps de chaque zone de police concernée. Dans le respect des conditions prévues à l'article 44/1, paragraphe 4, de la loi sur la fonction de police et en application de cet article, le chef de corps informe les autorités de police administrative compétentes.

Art. 22

Sur base du respect des principes d'adéquation, de pertinence et du caractère non excessif, dans le cadre de l'exercice de leurs missions respectives, et des finalités visées à l'article 5, alinéa 2, les services partenaires qui en application de l'article 16 disposent d'un droit d'interrogation dans la banque de données commune T.E.R. reçoivent l'évaluation de la menace en cas de confirmation de l'existence d'une entité validée dans la banque de données commune T.E.R.

Après réception de l'évaluation de la menace, le service partenaire qui a procédé à l'interrogation prend directement contact, par quelque moyen que ce soit, avec un des services de base en vue de contextualiser l'information disponible dans l'évaluation de la menace.

Art. 23

Aux fins de renforcer la prévention et la lutte contre le terrorisme et l'extrémisme pouvant mener au terrorisme, dans les limites visées à l'alinéa 2 et à l'article 24, une carte d'information peut être communiquée à une autorité ou une institution tierce dans le respect des principes d'adéquation, de pertinence et du caractère non excessif, et après évaluation par le gestionnaire, le responsable opérationnel et les services de base, sauf décision contraire du ministère public compétent lorsque la communication des données à caractères personnel et des informations judiciaires peut compromettre l'exercice de l'action publique ou la sécurité de personnes.

L'évaluation visée à l'alinéa 1^{er} porte au minimum sur:

instellingen, met uitzondering van de toezichhoudende overheden in het kader van hun opdrachten.

Art. 21

De creatie van een nieuwe entiteit in de gemeenschappelijke gegevensbank T.E.R. wordt onverwijld meegedeeld aan de voorzitter van de Lokale Task Force bedoeld in artikel 31 en de korpschef van elke betrokken politiezone. Met naleving van de voorwaarden bepaald in en met toepassing van artikel 44/1, paragraaf 4, van de wet op het politieambt informeert de korpschef de bevoegde bestuurlijke politieoverheden.

Art. 22

Op basis van de inachtneming van de principes van toereikendheid, relevantie en de niet-bovenmatige aard in het kader van de uitoefening van hun respectieve opdrachten en in het kader van de doeleinden van artikel 5, tweede lid, ontvangen de partnerdiensten die overeenkomstig artikel 16 over een vraagrecht in de gemeenschappelijke gegevensbank T.E.R. beschikken, de dreigingsevaluatie in geval van bevestiging van het bestaan van een gevalideerde entiteit in de gemeenschappelijke gegevensbank T.E.R.

Na ontvangst van de dreigingsevaluatie neemt de partnerdienst die tot de bevraging is overgegaan, met eender welk middel, direct contact op met een van de basisdiensten teneinde de in de dreigingsevaluatie beschikbare informatie te kunnen contextualiseren.

Art. 23

Met als doel de preventie en de bestrijding van het terrorisme en het extremisme dat tot terrorisme kan leiden, te versterken, binnen de grenzen bedoeld in het tweede lid en in artikel 24, kan, na evaluatie door de beheerder, de operationeel verantwoordelijke en de basisdiensten, een informatiekaart worden meegedeeld aan een derde overheid of instelling, met inachtneming van de principes van toereikendheid, relevantie en de niet-bovenmatige aard, behoudens andersluidende beslissing van het bevoegde Openbare Ministerie, wanneer de mededeling van persoonsgegevens en gerechtelijke informatie de uitoefening van de strafvordering of de veiligheid van personen in het gedrang kan brengen.

De in het eerste lid bedoelde evaluatie heeft ten minste betrekking op:

1° la contribution de l'autorité ou de l'institution tierce à la prévention ou à la lutte contre le terrorisme et l'extrémisme pouvant mener au terrorisme;

2° le traitement ultérieur qui sera réalisé par l'autorité ou l'institution tierce eu égard à l'exercice de ses compétences et les risques éventuels pour les libertés et droits fondamentaux de la personne concernée;

3° la situation de vulnérabilité de la personne concernée, en ce compris la minorité de la personne;

4° le caractère adéquat, pertinent et non excessif des catégories de données communiquées tenant compte du traitement ultérieur.

Le responsable opérationnel tient à la disposition des autorités de contrôle une liste à jour des communications visées à l'alinéa 1^{er} et l'évaluation visée à l'alinéa 2.

Art. 24

§ 1^{er}. La communication visée à l'article 23 s'effectue par la transmission, par quelque moyen sécurisé que ce soit, de la carte d'information relative aux entités validées.

Seuls les services de base sont autorisés à transmettre la carte d'information, sans préjudice des règles et procédures applicables pour leurs propres données à caractère personnel et informations.

§ 2. Les informations émanant de la carte d'information sont utilisées par le destinataire dans le cadre de ses propres compétences légales, sans que la carte d'information ne soit ni versée au dossier de l'entité validée ni communiquée à celle-ci.

Art. 25

§ 1^{er}. Seuls les services qui ont un droit de lecture et un droit d'écriture dans la banque de données commune T.E.R. sont autorisés à en extraire des listes de données à caractère personnel et d'informations de la carte d'information relative aux entités validées et ce, exclusivement pour un traitement interne. Cette extraction est effectuée par un membre du personnel titulaire d'une habilitation de sécurité "secret".

§ 2. La communication par un service de base, sous forme de listes, de données à caractère personnel ou

1° de bijdrage van de derde overheid of instelling tot de preventie en de bestrijding van het terrorisme en het extremisme dat tot terrorisme kan leiden;

2° de verdere verwerking die zal worden gedaan door de derde overheid of instelling rekening houdend met haar bevoegdheden en de eventuele risico's voor de fundamentele vrijheden en rechten van de betrokken persoon;

3° de kwetsbare toestand van de betrokken persoon, inclusief de minderjarigheid van de persoon;

4° het toereikende, ter zake dienende en niet overmatige karakter van de categorieën van meegedeelde gegevens rekening houdend met de verdere verwerking.

De operationeel verantwoordelijke houdt een geactualiseerde lijst van de in het eerste lid bedoelde mededelingen en de in het tweede lid bedoelde evaluatie ter beschikking van de toezichthoudende overheden.

Art. 24

§ 1. De mededeling bedoeld in artikel 23 gebeurt door het doorzenden, met eender welk beveiligd middel van de informatiekaart met betrekking tot de gevalideerde entiteiten.

Onverminderd de regels en de procedures die voor hun eigen persoonsgegevens en informatie van toepassing zijn, zijn enkel de basisdiensten gemachtigd om de informatiekaart door te zenden.

§ 2. De informatie die afkomstig is van de informatiekaart, wordt door de bestemming gebruikt in het kader van zijn eigen wettelijke bevoegdheden zonder dat de informatiekaart aan het dossier van de gevalideerde entiteit wordt toegevoegd of aan de gevalideerde entiteit wordt meegedeeld.

Art. 25

§ 1. Enkel de diensten met een leesrecht en een schrijfrecht in de gemeenschappelijke gegevensbank T.E.R. zijn gemachtigd om lijsten met persoonsgegevens en informatie van de informatiekaart met betrekking tot gevalideerde entiteiten uit de gegevensbank te halen, en zulks enkel voor interne verwerking. Deze extractie gebeurt door een personeelslid dat houder is van een veiligheidsmachtiging van het niveau "geheim".

§ 2. De mededeling aan andere diensten of instellingen door de basisdienst van persoonsgegevens of informatie

d'informations extraites des cartes d'information à d'autres services ou institutions n'est pas autorisée, sauf dans les cas prévus à l'article 23. Les listes ne peuvent être communiquées qu'aux autorités publiques et services publics. La finalité de la liste s'inscrit dans les missions légales du destinataire et est précisée et communiquée au destinataire de celle-ci. L'utilisation de la liste n'est autorisée que dans le cadre de la finalité précisée. Les listes ne peuvent pas être conservées pour une durée excédant celle nécessaire à la réalisation de la finalité pour laquelle elles sont obtenues.

Art. 26

§ 1^{er}. Le bourgmestre est destinataire de la carte d'information relative aux entités validées suivantes:

1° les *foreign terrorist fighters*, *homegrown terrorist fighters*, extrémistes potentiellement violents et les personnes condamnées pour terrorisme, qui ont établi leur résidence ou domicile dans sa commune, la fréquentent régulièrement ou y organisent régulièrement des activités;

2° les propagandistes de haine dont les effets sont perceptibles dans sa commune ou qui ont établi leur résidence ou leur domicile dans sa commune, la fréquentent régulièrement, y organisent ou y planifient d'organiser une ou plusieurs activités.

§ 2. Sans mettre en péril les impératifs opérationnels, le bourgmestre utilise, après un contact avec le chef de corps de la zone de police qui lui a transmis la carte d'information, les données à caractère personnel et informations émanant de celle-ci dans le cadre de ses compétences légales et sous sa propre responsabilité.

Art. 27

L'évaluation de la menace peut être utilisée par les services de base et les services partenaires dans le cadre de leurs propres compétences légales et conformément aux finalités de l'article 5, alinéa 2. L'évaluation de la menace peut être versée au dossier de l'entité moyennant la validation de l'Organe de coordination pour l'analyse de la menace.

L'Organe de coordination pour l'analyse de la menace actualise l'évaluation de la menace au minimum deux fois par an.

gehaald uit de informatiekaarten, onder de vorm van lijsten, wordt niet toegestaan, met uitzondering van de gevallen zoals voorzien in artikel 23. De lijsten kunnen enkel meegedeeld worden aan overheidsinstanties en openbare organen. De doelstelling van de lijst kadert binnen de wettelijke opdrachten van de ontvanger en wordt bepaald en meegedeeld aan de ontvanger van de lijst. Het gebruik van de lijst wordt enkel toegestaan in het kader van deze welbepaalde doelstelling. De lijsten mogen niet langer bewaard worden dan noodzakelijk is voor de verwezenlijking van de doelstelling waarvoor zij worden verkregen.

Art. 26

§ 1. De burgemeester is de bestemming van de informatiekaart betreffende de volgende gevalideerde entiteiten:

1° de *foreign terrorist fighters*, *homegrown terrorist fighters*, potentieel gewelddadige extremist en terrorismeveroordeelde die hun verblijfplaats of woonplaats in zijn gemeente hebben, zijn gemeente regelmatig bezoeken of er regelmatig activiteiten organiseren;

2° de haatpropagandisten van wie de effecten zichtbaar zijn in zijn gemeente of die hun verblijfplaats of woonplaats hebben in zijn gemeente, die zijn gemeente regelmatig bezoeken, of die er regelmatig een of meerdere activiteiten organiseren of plannen te organiseren.

§ 2. Zonder de operationele noodzaken in gevaar te brengen, en na contact met de korpschef van de politiezone die hem de informatiekaart toezond, gebruikt de burgemeester de persoonsgegevens en de informatie van de informatiekaart in het kader van zijn wettelijke bevoegdheden en onder zijn eigen verantwoordelijkheid.

Art. 27

De dreigingsevaluatie kan door de basisdiensten en de partnerdiensten worden gebruikt in het kader van hun eigen wettelijke bevoegdheden en overeenkomstig de doeleinden van artikel 5, tweede lid. De dreigingsevaluatie mag aan het dossier van de entiteit worden toegevoegd, onder voorbehoud van validatie door het Coördinatieorgaan voor de dreigingsanalyse.

Het Coördinatieorgaan voor de dreigingsanalyse werkt de dreigingsevaluatie ten minste tweemaal per jaar bij.

Art. 28

§ 1^{er}. Les services de base sont les seuls à pouvoir communiquer les données à caractère personnel et informations de la banque de données commune T.E.R., y compris sous forme de listes, dans le cadre de communications internationales visées aux paragraphes 2 et 3.

§ 2. Pour les missions visées à l'article 3, sans préjudice des règles internationales liant la Belgique, les données à caractère personnel et les informations de la banque de données commune T.E.R. peuvent être communiquées aux services de police étrangers et autorités judiciaires étrangères, aux organisations internationales de coopération judiciaire et policière et aux services de répression internationaux conformément à l'article 44/11/13 de la loi sur la fonction de police.

§ 3. Pour les missions visées à l'article 3, sans préjudice des règles internationales liant la Belgique, les données à caractère personnel et les informations de la banque de données commune T.E.R. peuvent être communiquées aux services de renseignement étrangers conformément à l'article 20, § 1^{er}, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Section 8

Protection des données

Art. 29

Dans le respect de l'exercice de leurs missions respectives, le contrôle du traitement des informations et des données à caractère personnel contenues dans la banque de données commune T.E.R., est assuré conjointement par les autorités de contrôle.

Elles peuvent à tout moment émettre les recommandations qu'elles estiment nécessaires pour les traitements réalisés dans la banque de données commune T.E.R.

Art. 30

§ 1^{er}. La responsabilité de la qualité des données à caractère personnel et des informations enregistrées dans la banque de données commune T.E.R. incombe:

1° au responsable du traitement propre à chaque service qui alimente la banque de données commune

Art. 28

§ 1. De basisdiensten zijn de enige diensten die de persoonsgegevens en de informatie van de gemeenschappelijke gegevensbank T.E.R. mogen meedelen, eveneens onder de vorm van lijsten, in het kader van de internationale communicatie bedoeld in paragrafen 2 en 3.

§ 2. Voor de opdrachten bedoeld in artikel 3, en onverminderd de internationale rechtsregels die België binden, kunnen de persoonsgegevens en de informatie van de gemeenschappelijke gegevensbank T.E.R. in overeenstemming met artikel 44/11/13 van de wet op het politieambt meegedeeld worden aan buitenlandse politiediensten en buitenlandse gerechtelijke autoriteiten, aan de internationale organisaties voor gerechtelijke en politionele samenwerking en aan de internationale rechtshandhavingdiensten.

§ 3. Voor de opdrachten bedoeld in artikel 3, en onverminderd de internationale rechtsregels die België binden, kunnen de persoonsgegevens en de informatie van de gemeenschappelijke gegevensbank T.E.R. in overeenstemming met artikel 20, § 1, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten worden meegedeeld aan buitenlandse inlichtingendiensten.

Afdeling 8

Gegevensbescherming

Art. 29

Met eerbied voor de uitoefening van hun respectievelijke bevoegdheden, wordt de controle op de verwerking van de in de gemeenschappelijke gegevensbank T.E.R., vervatte informatie en persoonsgegevens gezamenlijk verzekerd door de toezichthoudende overheden.

Zij kunnen op elk moment de aanbevelingen uitvaardigen die zij noodzakelijk achten voor de in de gemeenschappelijke gegevensbank T.E.R. uitgevoerde verwerkingen.

Art. 30

§ 1. De verantwoordelijkheid voor de kwaliteit van de persoonsgegevens en de informatie die geregistreerd zijn in de gemeenschappelijke gegevensbank T.E.R., komt toe aan:

1° de verwerkingsverantwoordelijke eigen aan elke dienst die de gemeenschappelijke gegevensbank T.E.R.

T.E.R. en ce qui concerne les données à caractère personnel et informations que ce service a transmises;

2° aux responsables du traitement visés à l'article 5, alinéa 1^{er}, en ce qui concerne les données à caractère personnel et informations validées sur les fiches de renseignements.

§ 2. Le responsable du traitement propre à chaque service qui alimente la banque de données commune T.E.R. veille à la légalité de la transmission de ses données à caractère personnel et informations vers la banque de données commune T.E.R.

§ 3. Le responsable du traitement visé à l'article 5, alinéa 1^{er}, veille notamment:

1° à la légalité de la transmission des données à caractère personnel et informations de la banque de données commune T.E.R.;

2° au bon fonctionnement technique et opérationnel de cette banque de données;

3° à l'intégrité, la disponibilité et la confidentialité des données à caractère personnel et informations de la banque de données commune T.E.R. et à la sécurité des systèmes d'accès.

Il détermine par directive les mesures nécessaires en vue de satisfaire à ces obligations.

§ 4. Le Roi peut, par arrêté délibéré en Conseil des ministres et après avis des autorités de contrôle, déterminer d'autres règles de responsabilité en matière de protection des données à caractère personnel des services de base et des services partenaires traitant ces données.

CHAPITRE 3

Enrichissement des données relatives aux entités et suivi d'une entité validée dans la banque de données commune T.E.R.

Art. 31

En vue d'assurer l'enrichissement des données à caractère personnel et informations relatives aux entités validées et aux entités en pré-enquêtes enregistrées dans la banque de données commune T.E.R. ainsi que le suivi et la prise de mesures à l'égard des entités validées dans la banque de données commune T.E.R., des données à caractère personnel et des informations

voedt voor wat de persoonsgegevens en informatie betreft die deze dienst heeft doorgezonden;

2° de verwerkingsverantwoordelijke bedoeld in artikel 5, eerste lid, voor wat de persoonsgegevens en informatie betreft die gevalideerd zijn op de inlichtingenfiches.

§ 2. De verwerkingsverantwoordelijke eigen aan elke dienst die de gemeenschappelijke gegevensbank T.E.R. voedt, waakt over de wettelijkheid van de doorzending van zijn persoonsgegevens en informatie naar de gemeenschappelijke gegevensbank T.E.R.

§ 3. De verwerkingsverantwoordelijke bedoeld in artikel 5 eerste lid waakt ondermeer over:

1° de wettelijkheid van de doorzending van de persoonsgegevens en informatie van de gemeenschappelijke gegevensbank T.E.R.;

2° de goede technische en operationele werking van deze gegevensbank;

3° de integriteit, de beschikbaarheid en de vertrouwelijkheid van de persoonsgegevens en informatie van de gemeenschappelijke gegevensbank T.E.R. en de veiligheid van de toegangssystemen.

Hij bepaalt bij richtlijn de noodzakelijke maatregelen met het oog op het verzekeren van deze verplichtingen.

§ 4. De Koning kan, bij een in Ministerraad overlegd besluit en na advies van de toezichthoudende overheden, andere regels bepalen inzake de verantwoordelijkheid op het gebied van de bescherming van persoonsgegevens van de basisdiensten en de partnerdiensten die deze gegevens verwerken.

HOOFDSTUK 3

Verrijking van gegevens over entiteiten en opvolging van een in de gemeenschappelijke gegevensbank T.E.R. gevalideerde entiteit

Art. 31

Met het oog op de verrijking van persoonsgegevens en informatie over de gevalideerde entiteiten en de entiteiten in vooronderzoek die zijn opgenomen in de gemeenschappelijke gegevensbank T.E.R. alsook de opvolging en het nemen van maatregelen ten aanzien van de in de gemeenschappelijke gegevensbank T.E.R. gevalideerde entiteiten, worden er in de gemeenschappelijke

enregistrées dans la banque de données commune T.E.R. ainsi que d'autres données à caractère personnel et informations pertinentes, y compris les informations classifiées au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, sont échangées au sein d'une ou plusieurs plateformes de concertation créées auprès de chaque arrondissement judiciaire, appelée Task force locale, dénommée ci-après "TFL", sauf si cet échange peut compromettre une enquête, l'exercice de l'action publique ou la sécurité de personnes.

La TFL est une structure de concertation au sens de l'article 458ter du Code pénal.

Art. 32

§ 1^{er}. La TFL est présidée par le directeur coordinateur administratif de la police fédérale ou son représentant.

Outre le président, la TFL se compose de représentants:

1° des services de renseignements et de sécurité;

2° de l'Organe de coordination pour l'analyse de la menace;

3° de la police fédérale et de la police locale;

4° de la Direction générale de l'Office des Étrangers du Service public fédéral Intérieur;

5° du Ministère public.

Le président et les participants à la TFL visés à l'alinéa 2, 1° à 4°, sont titulaires d'une habilitation de sécurité au moins du niveau "secret" en vertu des articles 4, alinéa 3, et 8 de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

Le président, en concertation avec les participants à la TFL visés à l'alinéa 2, 1° à 5°, peut inviter d'autres services, organes ou instances en raison de la contribution qu'ils peuvent apporter par leur fonction ou leurs compétences à un suivi ciblé et individualisé de l'entité.

Les services partenaires visés à l'article 2, 3°, l), seront représentés par un membre de l'administration centrale titulaire d'une habilitation de sécurité.

gegevensbank T.E.R. opgenomen persoonsgegevens en informatie, alsook andere relevante persoonsgegevens en informatie, waaronder geclassificeerde informatie in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, uitgewisseld binnen een of meer overlegplatformen die bij elk gerechtelijk arrondissement zijn opgericht, onder de naam "Lokale task force" (hierna "LTF"), tenzij die uitwisseling een onderzoek, de uitoefening van de strafvordering of de veiligheid van personen in het gedrang kan brengen.

De LTF is een overlegstructuur in de zin van artikel 458ter van het Strafwetboek.

Art. 32

§ 1. De LTF wordt voorgezeten door de bestuurlijke directeur-coördinator van de federale politie of zijn vertegenwoordiger.

Naast de voorzitter, is de LTF samengesteld uit vertegenwoordigers van:

1° de inlichtingen- en veiligheidsdiensten;

2° het Coördinatieorgaan voor de dreigingsanalyse;

3° de federale politie en de lokale politie;

4° de Algemene Directie Dienst Vreemdelingenzaken van de Federale overheidsdienst Binnenlandse Zaken;

5° het Openbaar Ministerie.

De voorzitter en de in het tweede lid, 1° tot 4°, bedoelde deelnemers van de LTF zijn houder van een veiligheidsmachtiging ten minste van het niveau "geheim" krachtens artikelen 4, derde lid, en 8 van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

In overleg met de in het tweede lid, 1° tot 5°, bedoelde deelnemers van de LTF kan de voorzitter andere diensten, organen of instanties uitnodigen wegens de bijdrage die ze door hun functie of bevoegdheden kunnen leveren aan een gerichte en geïndividualiseerde opvolging van de entiteit.

De in artikel 2, 3°, l), bedoelde partnerdiensten worden vertegenwoordigd door een lid van de centrale administratie met een veiligheidsmachtiging.

La coordination administrative, le secrétariat et le suivi de la TFL sont assurés par le directeur coordinateur ou les personnes qu'il désigne.

§ 2. Sans préjudice des compétences des services de base et des services partenaires, la TLF assure au moins les missions suivantes:

1° l'échange des données à caractère personnel et des informations visée à l'article 31 dans le cadre des missions visées à l'article 3;

2° le suivi des entités de la banque de données commune T.E.R. présentes sur son territoire;

3° la détermination de mesures appropriées pour chacune des entités validées.

Art. 33

§ 1^{er}. Dès la validation d'une entité dans la banque de données commune T.E.R., sur base des données à caractère personnel et des informations visées à l'article 31, la TFL, afin d'assurer le suivi de l'entité validée, se concerte systématiquement sur l'opportunité de prendre ou non une ou plusieurs mesures visées au paragraphe 2 à l'égard de l'entité validée, sans préjudice des prérogatives des autorités compétentes pour prendre ces mesures.

Dans le cadre du suivi d'une entité validée, lorsque des nouvelles données à caractère personnel et informations visée à l'article 31 peuvent entraîner un changement de mesures à son égard, la TFL procède à la concertation visée à l'alinéa premier.

En vue de l'élaboration de l'approche proactive, le résultat de la concertation visée aux alinéas 1 et 2 est transmis aux autorités compétentes pour prendre les éventuelles mesures à l'égard d'une entité validée dans la banque de données commune T.E.R. Le résultat de la concertation visée aux alinéas 1 et 2 relative à une entité validée est également enregistré dans la banque de données commune T.E.R. sauf si la mesure peut compromettre une enquête, l'exercice de l'action publique ou la sécurité de personnes ou qu'elle est classifiée au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

Sans préjudice de leurs prérogatives, les autorités compétentes pour prendre les mesures à l'égard d'une

De administratieve coördinatie, het secretariaat en de opvolging van de LTF worden gewaarborgd door de directeur-coördinator of de personen die hij aanwijst.

§ 2. Onverminderd de bevoegdheden van de basisdiensten en de partnerdiensten verzekert de LTF minstens de volgende opdrachten:

1° de uitwisseling van persoonsgegevens en informatie bedoeld in artikel 31 in het kader van de opdrachten bedoeld in artikel 3;

2° de opvolging van de entiteiten van de gemeenschappelijke gegevensbank T.E.R. die op het grondgebied van de LTF aanwezig zijn;

3° de bepaling van passende maatregelen voor elk van de gevalideerde entiteiten.

Art. 33

§ 1. Vanaf de validering van een entiteit in de gemeenschappelijke gegevensbank T.E.R., op grond van de persoonsgegevens en informatie bedoeld in artikel 31, pleegt de LTF, met het oog op de opvolging van de gevalideerde entiteit, stelselmatig overleg over de opportuniteit om al dan niet een of meer maatregelen bedoeld in paragraaf 2 ten aanzien van de gevalideerde entiteit te nemen, onverminderd de prerogatieven van de bevoegde overheden om deze maatregelen te nemen.

In het kader van de opvolging van een gevalideerde entiteit, wanneer nieuwe persoonsgegevens en informatie bedoeld in artikel 31 tot een wijziging van maatregelen ten aanzien van de entiteit kunnen leiden, gaat de LTF over tot het overleg bedoeld in het eerste lid.

Met het oog op de uitwerking van de proactieve aanpak wordt het resultaat van het in het eerste en tweede lid bedoelde overleg bezorgd aan de overheden die bevoegd zijn om eventuele maatregelen te nemen ten aanzien van een in de gemeenschappelijke gegevensbank T.E.R. gevalideerde entiteit. Het resultaat van het in het eerste en tweede lid bedoelde overleg met betrekking tot een gevalideerde entiteit wordt ook opgenomen in de gemeenschappelijke gegevensbank T.E.R., tenzij de maatregel een onderzoek, de uitoefening van de strafvordering of de veiligheid van personen in het gedrang kan brengen of tenzij de maatregel geclassificeerd is in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

Zonder afbreuk te doen aan hun prerogatieven, nemen de overheden die bevoegd zijn om maatregelen te

entité validée dans la banque de données commune prennent en considération le résultat de la concertation visée aux alinéas 1 et 2 lors de leur prise de décision.

§ 2. La TFL se concerte notamment sur les mesures suivantes, sauf si elles peuvent compromettre une enquête, l'exercice de l'action publique ou la sécurité de personnes:

1° la mesure de signalement et de désignation en application des dispositions en vigueur;

2° la suspension, le retrait et la restitution de cartes d'identification ou la suspension et le retrait d'autorisations qui relèvent du champ d'application de la loi du 19 juillet 1991 organisant la profession de détective privé et de la loi du 2 octobre 2017 réglementant la sécurité privée et particulière;

3° le retrait, la suspension ou la limitation d'autorisation ou d'agréments qui relèvent du champ d'application de la loi du 8 juin 2006 réglant les activités économiques et individuelles avec des armes;

4° le retrait d'habilitations, attestations et avis de sécurité qui relèvent du champ d'application de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité, attestations de sécurité et avis de sécurité;

5° la mise en place d'une enquête sociale et fiscale ou toute autre mesure spécifique dans les limites des compétences légales du Service d'information et de recherche sociale du Service public fédéral Emploi, Travail et Concertation Sociale;

6° la mise en place d'une enquête financière par la Cellule de Traitement des Informations Financières conformément à l'article 81, paragraphe 2, et l'article 83, paragraphe 2, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces;

7° la prise de mesures spécifiques dans les limites des compétences légales des services de l'Office National de l'Emploi (ONEm), l'Office wallon de la formation professionnelle et de l'emploi (FOREm), l'Office régional bruxellois de l'Emploi (Actiris), Bruxelles formation, le *Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding* (VDAB) et l'*Arbeitsamt der Deutschsprachigen Gemeinschaft Belgiens* (ADG);

nemen ten aanzien van een in de gemeenschappelijke gegevensbank gevalideerde entiteit, het resultaat van het in het eerste en tweede lid bedoelde overleg in overweging bij het nemen van hun beslissing.

§ 2. De LTF pleegt inzonderheid overleg over de volgende maatregelen, tenzij deze een onderzoek, de uitoefening van de strafvordering of de veiligheid van personen in het gedrang kunnen brengen:

1° de maatregel van seining en ontseining met toepassing van de inwerking zijnde bepalingen;

2° de schorsing, de intrekking en de teruggave van identificatiekaarten of de schorsing en de intrekking van vergunningen die behoren tot het toepassingsgebied van de wet van 19 juli 1991 tot regeling van het beroep van privédetective en de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid;

3° de intrekking, de schorsing of de beperking van de vergunningen of de erkenningen die behoren tot het toepassingsgebied van de wet van 8 juni 2006 houdende de regeling van economische en individuele activiteiten met wapens;

4° de intrekking van veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen die behoren tot het toepassingsgebied van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

5° de uitvoering van een sociaal en fiscaal onderzoek of enige andere specifieke maatregel binnen de grenzen van de wettelijke bevoegdheden van de Sociale Inlichtingen- en Opsporingsdienst van de Federale Overheidsdienst Werkgelegenheid, Arbeid en Sociaal Overleg;

6° de uitvoering van een financieel onderzoek door de Cel voor Financiële Informatieverwerking overeenkomstig artikel 81, paragraaf 2, en artikel 83, paragraaf 2, van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;

7° het nemen van specifieke maatregelen binnen de grenzen van de wettelijke bevoegdheden van de diensten van de de Rijksdienst voor Arbeidsvoorziening (RVA), l'*Office wallon de la formation professionnelle et de l'emploi* (FOREm), het Brusselse Gewestelijke Dienst voor Arbeidsbemiddeling (Actiris), Bruxelles formation, de *Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding* (VDAB) en de *Arbeitsamt der Deutschsprachigen Gemeinschaft Belgiens* (ADG);

8° la prise de mesures spécifiques par l'Office des Étrangers en matière d'accès au territoire, de séjour, d'établissement et d'éloignement;

9° le refus, le retrait ou l'invalidation de passeport ou d'un titre de voyage belge et de documents d'identité belge conformément au Code consulaire;

10° l'inscription d'office ou la radiation d'office des registres de la population conformément à la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour;

11° le gel des avoirs en application de l'arrêté royal du 28 décembre 2006 relatif aux mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le financement du terrorisme;

12° le suivi effectué par les services de police dans le cadre des missions visées aux articles 14 et 15, de la loi sur la fonction de police;

13° le suivi effectué par les services de renseignements dans le cadre des missions visées aux articles 7 et 11 de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité;

14° le suivi des médias sociaux de l'entité concernée;

15° les mesures visées par le règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne et le règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).

8° het nemen van specifieke maatregelen door de Dienst Vreemdelingenzaken op het gebied van toegang tot het grondgebied, verblijf, vestiging en verwijdering;

9° de weigering, de intrekking of de ongeldigverklaring van een Belgisch paspoort of reisdocument en van Belgische identiteitsdocumenten overeenkomstig het Consulair Wetboek;

10° de ambtshalve inschrijving of schrapping uit de bevolkingsregisters overeenkomstig de wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten;

11° de bevrozing van de tegoeden met toepassing van het koninklijk besluit van 28 december 2006 inzake specifieke beperkende maatregelen tegen bepaalde personen en entiteiten met het oog op de strijd tegen de financiering van het terrorisme;

12° de opvolging uitgevoerd door de politiediensten in het kader van de opdrachten bedoeld in de artikelen 14 en 15 van de wet op het politieambt;

13° de opvolging uitgevoerd door de inlichtingendiensten in het kader van de opdrachten bedoeld in de artikelen 7 en 11 van de organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

14° de opvolging van de sociale media van de betrokken entiteit;

15° de maatregelen bedoeld in Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud en de Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (digitaaldienstenverordening).

CHAPITRE 4

Dispositions modificatives

Section 1^{er}

Dispositions modificatives de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

Art. 34

À l'article 11, paragraphe 1^{er}, 2°, de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, les mots "à l'article 44/11/3^{ter} §§ 2 et 3, et à l'article 44/11/3^{quater} de la loi du 5 août 1992 sur la fonction de police" sont remplacés par les mots "aux articles 16 et 23, de la loi du [DATE] portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police".

Art. 35

Le sous-titre 4, du Titre 3, de la même loi, est complété par les mots "et dans la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation"".

Art. 36

L'article 138, paragraphe 2, de la même loi, est complété par les 8°, 9° et 10° rédigés comme suit:

"8° "la loi du [DATE] portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.")": la loi du [DATE] portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police;

HOOFDSTUK 4

Wijzigingsbepalingen

Afdeling 1

Wijzigingsbepalingen van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens

Art. 34

In artikel 11, paragraaf 1, 2°, van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, worden de woorden "in artikel 44/11/3^{ter}, §§ 2 en 3, en artikel 44/11/3^{quater} van de wet van 5 augustus 1992 op het politieambt" vervangen door de woorden "in de artikelen 16 en 23, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.") en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt".

Art. 35

De ondertitel 4, van titel 3, van dezelfde wet, wordt aangevuld met de woorden "en de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces"".

Art. 36

Artikel 138, paragraaf 2, van dezelfde wet, wordt aangevuld met de bepalingen onder 8°, 9° en 10°, luidende:

"8° "de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.")": de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R."). en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt;

9° “la banque de données commune ”T.E.R.””: la banque de données visées à l’article 3 de la loi du [DATE] portant création de la banque de données commune “Terrorisme, Extrémisme, processus de Radicalisation” (“T.E.R.”);

10° “les responsables conjoints du traitement de la banque de données commune ”T.E.R.””: les responsables du traitement visés à l’article 5, alinéa 1^{er}, de la loi du [DATE] portant création de la banque de données commune “Terrorisme, Extrémisme, processus de Radicalisation” (“T.E.R.”).

Art. 37

L’article 139, alinéa 1^{er}, de la même loi, est complété par les mots “et à tout traitement de données à caractère personnel dans la banque de données commune ”T.E.R.”.

Art. 38

L’article 140 de la même loi est complété par un 5° rédigé comme suit:

“5° lorsque le traitement est utile dans le cadre des finalités prévues à l’article 5, alinéa 2, de la loi du [DATE] portant création de la banque de données commune “Terrorisme, Extrémisme, processus de Radicalisation” (“T.E.R.”).”.

Art. 39

À l’article 143 de la même loi, les mots “l’article 44/11/3bis de la loi de 5 août 1992 sur la fonction de police en ce qui concerne les banques de données communes dont l’OCAM est le gestionnaire opérationnel.” sont remplacés par les mots “l’article 7 de la loi du [DATE] portant création de la banque de données commune “Terrorisme, Extrémisme, processus de Radicalisation” (“T.E.R.”) en ce qui concerne la banque de données commune “T.E.R.”.”.

Art. 40

À l’article 147 de la même loi, les mots “, les responsables conjoints du traitement de la banque de données commune “T.E.R.”” sont insérés entre les mots “l’article 161” et les mots “et l’OCAM”.

9° “de gemeenschappelijke gegevensbank ”T.E.R.””: de gegevensbank bedoeld in artikel 3 van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”);

10° “de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank ”T.E.R.””: de verwerkingsverantwoordelijken bedoeld in artikel 5, eerste lid, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”).

Art. 37

Artikel 139, eerste lid, van dezelfde wet, wordt aangevuld met de woorden “en op elke verwerking van persoonsgegevens in de gemeenschappelijke gegevensbank ”T.E.R.”.”.

Art. 38

Artikel 140 van dezelfde wet, wordt aangevuld met een bepaling onder 5°, luidende:

“5° wanneer de verwerking nuttig is in het kader van de doeleinden bedoeld in artikel 5, tweede lid, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”).”.

Art. 39

In artikel 143 van dezelfde wet, worden de woorden “artikel 44/11/3bis van de wet van 5 augustus 1992 op het politieambt voor wat betreft de gemeenschappelijke gegevensbanken waarvan het OCAD de operationele beheerder is.” vervangen door de woorden “artikel 7 van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”) voor wat betreft de gemeenschappelijke gegevensbank “T.E.R.”.”.

Art. 40

In artikel 147 van dezelfde wet, worden de woorden “de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank ”T.E.R.”” ingevoegd tussen de woorden “artikel 161” en de woorden “en het OCAD”.

Art. 41

L'article 149, 2°, de la même loi est complété par les mots "ou dans le cadre des finalités de la banque de données commune "T.E.R." visées à l'article 5, alinéa 2, de la loi du [DATE] portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.")".

Art. 42

À l'article 155 de la même loi, le paragraphe 1^{er} est remplacé comme suit:

"§ 1^{er}. Sous réserve des dispositions de l'article 13 de la loi du [DATE] portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R."), en cas de brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement concerné la notifie à l'autorité de contrôle compétente dans les meilleurs délais et si possible, 72 heures après en avoir pris connaissance."

Art. 43

À l'article 156, paragraphe 1^{er}, de la même loi, les modifications suivantes sont apportées:

1° à l'alinéa 1^{er}, les mots "de la banque de données commune "T.E.R."", sont insérés entre les mots "de la loi du 11 décembre 1998," et les mots "des banques de données de l'OCAM";

2° à l'alinéa 2, la phrase liminaire du 1° est remplacée comme suit:

"1° pour la banque de données commune "T.E.R." et les banques de données de l'OCAM:".

Art 44

Dans le Titre 3, sous-titre 4, chapitre 7, section 5, de la même loi, il est inséré un article 157/1, rédigé comme suit:

"Art. 157/1. § 1^{er}. Les responsables conjoints du traitement de la banque de données commune "T.E.R." et, le cas échéant, le sous-traitant désignent un délégué à la protection des données. Cette décision est communiquée aux autorités de contrôle compétentes.

Art. 41

Artikel 149, 2°, van dezelfde wet, wordt aangevuld met de woorden "of in het kader van de doeleinden van de gemeenschappelijke gegevensbank "T.E.R." bedoeld in artikel 5, tweede lid, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.")".

Art. 42

In artikel 155 van dezelfde wet, wordt de paragraaf 1 vervangen als volgt:

"§ 1. Onder voorbehoud van de bepalingen van artikel 13 van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.") meldt de betrokken verwerkingsverantwoordelijke een inbreuk op de beveiliging die een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt, binnen de kortste termijn en indien mogelijk 72 uur nadat hij er kennis van heeft genomen, aan de bevoegde toezichthoudende overheid."

Art. 43

In artikel 156, paragraaf 1, van dezelfde wet, worden de volgende wijzigingen aangebracht:

1° in het eerste lid, worden de woorden "van de gemeenschappelijke gegevensbank "T.E.R."", ingevoegd tussen de woorden "van de wet van 11 december 1998," en de woorden "van de gegevensbanken van het OCAD";

2° in het tweede lid, wordt de inleidende zin van de bepaling onder 1° vervangen als volgt:

"1° voor de gemeenschappelijke gegevensbank "T.E.R." en de gegevensbanken van het OCAD:".

Art. 44

In titel 3, ondertitel 4, hoofdstuk 7, afdeling 5, van dezelfde wet, wordt een artikel 157/1 ingevoegd, luidende:

"Art. 151/1. § 1. De gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R.", en desgevallend de verwerker, wijzen een functionaris voor gegevensbescherming aan. Deze beslissing wordt meegedeeld aan de bevoegde toezichthoudende autoriteiten.

Le délégué à la protection des données est titulaire d'une habilitation de sécurité de niveau "secret", au sens de la loi du 11 décembre 1998.

§ 2. Le délégué à la protection des données ne peut pas être sanctionné en raison de l'exercice de ses fonctions. Il ne peut pas non plus être relevé de ses fonctions en raison de l'exercice de ses missions, sauf s'il a commis une faute grave ou s'il ne remplit plus les conditions nécessaires à l'exercice de ses fonctions.

Le délégué à la protection des données peut s'adresser à l'Organe de contrôle de l'information policière ou au Comité permanent R pour contester cette décision.

§ 3. Il est chargé de manière indépendante:

1° de veiller au respect du présent sous-titre lors de tout traitement de données à caractère personnel dans le cadre de la banque de données commune "T.E.R.";

2° de conseiller toutes mesures utiles afin d'assurer la sécurité des données enregistrées dans la banque de données commune "T.E.R.";

3° d'informer et conseiller les responsables conjoints du traitement de la banque de données commune "T.E.R.", et le cas échéant, le gestionnaire, le responsable opérationnel, le sous-traitant, le dirigeant et le personnel du service concerné procédant au traitement sur les obligations qui leur incombent sur la base du présent sous-titre et de la loi du [DATE] portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.");

4° de fournir des avis ou des recommandations aux responsables conjoints du traitement de la banque de données commune "T.E.R.", et le cas échéant, au gestionnaire, au responsable opérationnel et au sous-traitant;

5° d'exécuter d'autres missions qui lui sont confiées par les responsables conjoints du traitement de la banque de données commune "T.E.R.", et le cas échéant, le responsable opérationnel;

§ 4. Le délégué à la protection des données:

1° veille à la sensibilisation des utilisateurs dans les matières de protection des données à caractère personnel et de sécurité;

De functionaris voor gegevensbescherming is titularis van een veiligheidsmachtiging "geheim", in de zin van de wet van 11 december 1998.

§ 2. De functionaris voor gegevensbescherming kan niet gestraft worden voor het uitoefenen van zijn functie. Hij kan evenmin van zijn functie ontheven worden omwille van de uitvoering van zijn opdrachten, behalve indien hij een zware fout heeft begaan of de voorwaarden noodzakelijk voor het uitoefenen van zijn functie niet langer vervult.

De functionaris voor gegevensbescherming kan zich tot het Controleorgaan op de Politie Informatie of het Vast Comité I wenden om deze beslissing aan te vechten.

§ 3. Hij is, op een onafhankelijke wijze, belast met:

1° het toezien op de naleving van deze ondertitel bij elke verwerking van persoonsgegevens in het kader van de gemeenschappelijke gegevensbank "T.E.R.";

2° het adviseren over alle nuttige maatregelen ten einde de veiligheid van de opgeslagen gegevens in de gemeenschappelijke gegevensbank "T.E.R." te verzekeren;

3° het informeren en adviseren van de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R.", en desgevallend de beheerder, de operationeel verantwoordelijke, de verwerker, het diensthoofd en de personeelsleden van de betrokken dienst die de verwerking verrichten over hun verplichtingen op grond van deze ondertitel en de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.");

4° het verstrekken van adviezen of aanbevelingen aan de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R.", en desgevallend aan de beheerder, de operationeel verantwoordelijke en de verwerker;

5° het uitvoeren van andere opdrachten die hem door de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R.", en in voorkomend geval de operationeel verantwoordelijke.

§ 4. De functionaris voor gegevensbescherming:

1° waakt over de bewustmaking van de gebruikers inzake bescherming van de persoonsgegevens en de veiligheid;

2° coopère avec le gestionnaire dans le cadre de l'élaboration des procédures;

3° coopère, si nécessaire avec les délégués à la protection des données des services qui traitent des données de la banque de données commune "T.E.R.";

4° est le point de contact avec les autorités de contrôle sur les questions relatives aux traitements réalisés dans la banque de données commune "T.E.R.".

§ 5. Le délégué à la protection des données exerce ses fonctions en toute indépendance et dans le respect des compétences et missions respectives des services de base et des services partenaires.

Les responsables conjoints du traitement de la banque de données commune T.E.R., le gestionnaire et le responsable opérationnel veillent à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

Les responsables conjoints du traitement de la banque de données commune T.E.R. veillent à ce que le délégué à la protection des données dispose des ressources nécessaires pour exercer ses missions.

Le délégué à la protection des données peut être assisté par un ou plusieurs adjoints.

Il rend compte directement aux responsables conjoints du traitement de la banque de données commune T.E.R. qui en informent le responsable opérationnel.

§ 6. Le cas échéant, les modalités de fonctionnement, de désignation ainsi que les compétences requises du délégué à la protection des données peuvent être définies par le Roi."

Art. 45

L'article 158 de la même loi est remplacé comme suit:

"Art. 158. Par dérogation aux articles 20, 22, 23, 58 et 59 de la présente loi et aux articles 35 et 36 du Règlement, un protocole, un avis du délégué à la protection des données, une analyse d'impact relative à la protection des données et l'avis résultant de la consultation de l'autorité de contrôle compétente ne

2° werkt samen met de beheerder in het kader van het uitwerken van procedures;

3° werkt, indien nodig, samen met de functionarissen voor de gegevensbescherming van de diensten die de gegevens in de gemeenschappelijke gegevensbank "T.E.R." verwerken;

4° is de contactpersoon met de toezichthoudende autoriteiten voor aangelegenheden in verband met de verwerkingen die in de gemeenschappelijke gegevensbank "T.E.R." worden uitgevoerd.

§ 5. De functionaris voor gegevensbescherming oefent zijn functies uit in alle onafhankelijkheid en met inachtneming van de respectieve bevoegdheden en opdrachten van de basisdiensten en de partnerdiensten.

De gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R.", de beheerder en de operationeel verantwoordelijke zien erop toe dat de functionaris voor gegevensbescherming tijdig en op passende wijze betrokken wordt bij alle aangelegenheden in verband met de bescherming van persoonsgegevens.

De gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R." ziet erop toe dat de functionaris voor gegevensbescherming beschikt over de nodige middelen voor het vervullen van zijn opdrachten.

De functionaris voor gegevensbescherming kan worden bijgestaan door een of meer adjuncten.

Hij brengt rechtstreeks verslag uit aan de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R.", die de operationeel verantwoordelijke op de hoogte brengen.

§ 6. Desgevallend kunnen nadere regels voor de werking, de aanwijzing en de vereiste bevoegdheden van de functionaris voor gegevensbescherming door de Koning worden bepaald."

Art. 45

Artikel 158 van dezelfde wet wordt vervangen als volgt:

"Art. 158. In afwijking van de artikelen 20, 22, 23, 58 en 59 van deze wet en van de artikelen 35 en 36 van de Verordening kan noch een protocol, noch een advies van de functionaris voor gegevensbescherming, noch een gegevensbeschermingseffectbeoordeling, noch het advies volgend op de raadpleging van de

peuvent pas être exigés comme condition préalable à la communication de données à caractère personnel entre l'OCAM et tout organisme public ou privé dans l'intérêt de l'exercice des missions de l'OCAM.

Par dérogation aux articles 20, 22, 23, 58 et 59 de la présente loi et aux articles 35 et 36 du Règlement, un protocole, un avis du délégué à la protection des données, une analyse d'impact relative à la protection des données et l'avis résultant de la consultation de l'autorité de contrôle compétente ne peuvent pas être exigés comme condition préalable à la communication de données à caractère personnel issues de la banque de données commune "T.E.R." à tout organisme public ou privé dans l'intérêt de l'exercice des missions de prévention et de suivi du terrorisme et de l'extrémisme, lorsqu'il peut mener au terrorisme, visées à l'article 3, alinéa 1^{er}, de la loi du [DATE] portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.").

La communication visée à l'alinéa 1^{er} se déroule conformément aux articles 8 à 12 de la loi du 10 juillet 2006.

La communication visée à l'alinéa 2 se déroule conformément aux articles 20 à 28 de la loi du [DATE] portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.").

Par dérogation à l'article 20, paragraphe 1^{er}, alinéa 2, lorsque les parties décident de conclure un protocole, celui-ci comprend:

1° l'identification de l'organisme public ou privé qui échangent les données à caractère personnel et, le cas échéant, l'identification de l'OCAM;

2° l'identification des responsables du traitement;

3° les coordonnées des délégués à la protection des données concernés;

4° les finalités pour lesquelles les données à caractère personnel sont transférées;

5° la base légale;

6° les restrictions aux droits de la personne concernée.

Le protocole visé à l'alinéa 5 porte le marquage "DIFFUSION RESTREINTE" au sens de l'arrêt royal du 24 mars 2000 portant exécution de la loi

bevoegde toezichhoudende autoriteit vereist worden als voorafgaande voorwaarde voor de mededeling van persoonsgegevens tussen het OCAD en enig openbaar of particulier orgaan, in het belang van de uitvoering van de opdrachten van het OCAD.

In afwijking van de artikelen 20, 22, 23, 58 en 59 van deze wet en van de artikelen 35 en 36 van de Verordening kan noch een protocol, noch een advies van de functionaris voor gegevensbescherming, noch een gegevensbeschermingseffectbeoordeling, noch het advies volgend op de raadpleging van de bevoegde toezichhoudende autoriteit vereist worden als voorafgaande voorwaarde voor de mededeling van persoonsgegevens van de gemeenschappelijke gegevensbank "T.E.R." aan enig openbaar of particulier orgaan, in het belang van de uitvoering van de opdrachten inzake de voorkoming en de opvolging van terrorisme en extremisme, dat kan leiden tot terrorisme, bedoeld in artikel 3, eerste lid, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.").

De mededeling bedoeld in het eerste lid vindt plaats in overeenstemming met de artikelen 8 tot 12 van de wet van 10 juli 2006.

De mededeling bedoeld in het tweede lid vindt plaats in overeenstemming met de artikelen 20 tot 28 van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.").

Wanneer de partijen beslissen een protocol af te sluiten, bevat dit, in afwijking van artikel 20, paragraaf 1, tweede lid, het volgende:

1° de identificatie van het openbaar of particulier orgaan die de persoonsgegevens uitwisselen, en in voorkomend geval, de identificatie van het OCAD;

2° de identificatie van de verwerkingsverantwoordelijken;

3° de contactgegevens van de betrokken functionarissen voor gegevensbescherming;

4° de doeleinden waarvoor de persoonsgegevens worden doorgegeven;

5° de wettelijke grondslag;

6° de beperkingen van de rechten van de betrokkene.

Het protocol bedoeld in het vijfde lid draagt de markering "BEPERKTE VERSPREIDING" in de zin van het koninklijk besluit van 24 maart 2000 tot uitvoering van

du 11 décembre 1998, pour autant qu'une classification au sens de la loi du 11 décembre 1998 ne se justifie pas.”.

Art. 46

L'article 161 de la même loi est complété par un alinéa 2, rédigé comme suit:

“Les autorités de contrôle visées à l'article 2, 2^o, de la loi du [DATE] portant création de la banque de données commune “Terrorisme, Extrémisme, processus de Radicalisation” (“T.E.R.”) sont désignées conjointement comme autorités de protection des données chargées du contrôle du traitement des données à caractère personnel dans la banque de données commune “T.E.R.”.”.

Art. 47

L'article 162 de la même loi est complété par deux alinéas rédigés comme suit:

“Par dérogation à l'alinéa 1^{er}, la consultation à des fins historiques, scientifiques ou statistiques des données à caractère personnel relatives aux entités enregistrées dans la banque de données commune T.E.R. par un responsable du traitement ultérieur est autorisée par le responsable opérationnel de la banque de données commune “T.E.R.” après concertation avec les services de base visés à l'article 2, 2^o, de la loi du [DATE] portant création de la banque de données commune “Terrorisme, Extrémisme, processus de Radicalisation” (“T.E.R.”). Lorsqu'elle peut compromettre la sécurité d'une personne, l'exercice de l'action publique, l'exercice d'une enquête de renseignement ou la relation avec un service répressif d'un État étranger ou avec un service de renseignement et de sécurité d'un État étranger, la consultation est d'office refusée.

Toute demande adressée aux Archives de l'État de traitement ultérieur de données à caractère personnel enregistrées dans la banque de données commune “T.E.R.” à d'autres fins que celles visées à l'alinéa 3 est refusée à moins que la finalité soit légitime, qu'il n'y ait pas une atteinte disproportionnée à la vie privée et après avis du responsable opérationnel.”.

Art. 48

À l'article 164 de la même loi, les modifications suivantes sont apportées:

de la wet van 11 december 1998, voor zover een classificatie in de zin van de wet van 11 december 1998 niet gerechtvaardigd is.”.

Art. 46

Artikel 161 van dezelfde wet wordt aangevuld met een tweede lid, luidende:

“De toezichthoudende overheden bedoeld in artikel 2, 2^o, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”) worden gezamenlijk aangewezen als gegevensbeschermingsautoriteiten belast met de controle van de verwerking van persoonsgegevens in de gemeenschappelijke gegevensbank “T.E.R.”.”.

Art. 47

Artikel 162 van dezelfde wet wordt aangevuld met twee leden, luidende:

“In afwijking van het eerste lid, wordt de raadpleging voor historische, wetenschappelijke of statistische doeleinden, door een verdere verwerkingsverantwoordelijke, van persoonsgegevens met betrekking tot de in de gemeenschappelijke gegevensbank “T.E.R.” geregistreerde entiteiten toestaan door de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank “T.E.R.” na overleg met de basisdiensten bedoeld in artikel 2, 2^o van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”). Wanneer de raadpleging de veiligheid van een persoon, de uitoefening van de strafvordering, de uitoefening van een inlichtingenonderzoek of de relatie met een rechtshandavingsinstantie van een buitenlandse Staat of met een inlichtingen- en veiligheidsdienst van een buitenlandse Staat in het gedrang kan brengen, wordt ze automatisch geweigerd.

Elke vraag aan de Rijksarchieven om verdere verwerking van persoonsgegevens geregistreerd in de gemeenschappelijke gegevensbank “T.E.R.” voor overige doelen dan die bedoeld in het derde lid wordt geweigerd tenzij het doel legitiem is, er geen onevenredige afbreuk wordt gedaan aan het privéleven en na advies van de operationeel verantwoordelijke.”.

Art. 48

In atikel 164 van dezelfde wet, worden de volgende wijzigingen aangebracht:

1° à l'alinéa 2, les mots "ou le responsable opérationnel de la banque de données commune "T.E.R." après concertation avec les services de base visés à l'article 2, 2°, de la loi du [DATE] portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") pour ce qui concerne la banque de données commune "T.E.R."" sont insérés entre les mots "l'OCAM" et les mots "peut autoriser la consultation de données pseudonymisées";

2° à l'alinéa 3, les mots "ou le responsable opérationnel de la banque de données commune "T.E.R." après concertation avec les services de base visés à l'article 2, 2°, de la loi du [DATE] portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") pour ce qui concerne la banque de données commune "T.E.R."" sont insérés entre les mots "l'OCAM" et les mots "refuse la consultation";

3° à l'alinéa 4, les mots "ou le responsable opérationnel de la banque de données commune "T.E.R." après concertation avec les services de base visés à l'article 2, 2°, de la loi du [DATE] portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") pour ce qui concerne la banque de données commune "T.E.R."" sont insérés entre les mots "l'OCAM" et les mots "peut autoriser la consultation de données non pseudonymisées".

Art. 49

À l'article 165 de la même loi, les mots "ou le responsable opérationnel de la banque de données commune "T.E.R." après concertation avec les services de base visés à l'article 2, 2°, de la loi du [DATE] portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" ("T.E.R.") pour ce qui concerne la banque de données commune "T.E.R."" sont insérés entre les mots "avec l'accord de l'OCAM" et les mots "et sous les conditions que celui-ci aura fixées".

Art. 50

À l'article 166, alinéa 3, de la même loi, les 4° et 5° sont complétés par les mots "ou par le responsable opérationnel de la banque de données commune "T.E.R." après concertation avec les services de base visés à l'article 2, 2°, de la loi du [DATE] portant création de la banque de données commune "Terrorisme, Extrémisme,

1° in het tweede lid, worden de woorden "of de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank "T.E.R." na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R."), wat betreft de gemeenschappelijke gegevensbank "T.E.R.," ingevoegd tussen de woorden "het OCAD" en de woorden "de raadpleging van gepseudonimiseerde gegevens toestaan";

2° in het derde lid, worden de woorden "of de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank "T.E.R." na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R."), wat betreft de gemeenschappelijke gegevensbank "T.E.R.," ingevoegd tussen de woorden "weigert het OCAD" en de woorden "de raadpleging";

3° in het vierde lid, worden de woorden "of de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank "T.E.R." na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R."), wat betreft de gemeenschappelijke gegevensbank "T.E.R.," ingevoegd tussen de woorden "kan het OCAD" en de woorden "de raadpleging van niet-gepseudonimiseerde gegevens toestaan".

Art. 49

In artikel 165 van dezelfde wet, worden de woorden "of de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank "T.E.R." na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R."), wat betreft de gemeenschappelijke gegevensbank "T.E.R.," ingevoegd tussen de woorden "met het akkoord van het OCAD" en de woorden "en onder de voorwaarden die het vastlegt".

Art. 50

In artikel 166, derde lid, van dezelfde wet, worden de bepalingen onder 4° en 5° aangevuld met de woorden "of door de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank "T.E.R." na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van [DATUM] tot oprichting van

processus de Radicalisation” (“T.E.R.”) pour ce qui concerne la banque de données commune “T.E.R.””.

Section 2

Disposition modificative de la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d’extrémisme et de terrorisme

Art. 51

À l’article 4 de la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d’extrémisme et de terrorisme, les modifications suivantes sont apportées:

1° dans le paragraphe 1^{er}, les mots “l’article 1^{er}, 15°, de l’arrêté royal du 23 avril 2018 relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1^{re} bis “de la gestion des informations” du chapitre IV de la loi sur la fonction de police et à l’article 1^{er}, 12°, de l’arrêté royal du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters,” sont remplacés par les mots “l’article 2, 17°, de la loi du [DATE] portant création de la banque de données commune “Terrorisme, Extrémisme, processus de Radicalisation” (“T.E.R.”) et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d’extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police”;

2° dans le paragraphe 2, les mots “à l’article 44/11/3^{ter}, § 1^{er}, de la loi du 5 août 1992 sur la fonction de police” sont remplacés par les mots “à l’article 2, 2° et 22°, de la loi du [DATE] portant création de la banque de données commune “Terrorisme, Extrémisme, processus de Radicalisation” (“T.E.R.”) et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d’extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police”.

de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”), wat betreft de gemeenschappelijke gegevensbank “T.E.R.””.

Afdeling 2

Wijzigingsbepaling van de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme

Art. 51

In artikel 4 van de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, worden de woorden “artikel 1, 15°, van het koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1bis “het informatiebeheer” van hoofdstuk IV van de wet op het politieambt en artikel 1, 12°, van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Terrorist Fighters,” vervangen door de woorden “artikel 2, 17°, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”) en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt”;

2° in paragraaf 2, worden de woorden “artikel 44/11/3^{ter}, § 1, van de wet van 5 augustus 1992 op het politieambt” vervangen door de woorden “artikel 2, 2° en 22°, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”) en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt”.

Section 3*Dispositions modificatives de la loi du 5 août 1992
sur la fonction de police***Art. 52**

Dans le chapitre IV, section 12, sous-section 8, de la loi du 5 août 1992 sur la fonction de police, insérée par la loi du 18 mars 2014 et modifiée en dernier lieu par la loi du 31 juillet 2020, il est inséré un article 44/11/9bis, rédigé comme suit:

“Art. 44/11/9bis. Lorsque dans leurs missions de police administrative ou de police judiciaire, les membres des services de police sont appelés à coopérer avec les services de la santé, d’urgence et/ou de secours, ils peuvent communiquer des données à caractère personnel et des informations pour autant qu’elles soient adéquates, pertinentes et strictement nécessaires pour permettre aux membres des services de la de santé, d’urgence et/ou de secours, d’effectuer leurs missions dans des conditions de sécurité optimales et d’assurer la sécurité et l’intégrité psychologique et physique de toute personne dans l’exercice de ces fonctions.”

Section 4*Dispositions modificatives du Code consulaire***Art. 53**

À l’article 39/4, alinéa 3, du Code consulaire, inséré par la loi du 3 juillet 2019, les mots “l’article 6, § 1^{er}, 1° ou 1°/1, de l’arrêté royal du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters” sont remplacés par les mots “l’article 2, 7° ou 8°, de la loi du [DATE] portant création de la banque de données commune “Terrorisme, Extrémisme, processus de Radicalisation” (“T.E.R.”) et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d’extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police”.

Art. 54

À l’article 65/1, alinéa 3, du même Code, inséré par la loi du 3 juillet 2019, les mots “l’article 6, § 1^{er}, 1° ou 1°/1, de l’arrêté royal du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters” sont remplacés par les mots “l’article 2, 7° ou 8°, de la loi du [DATE] portant

Afdeling 3*Wijzigingsbepalingen van de wet van 5 augustus 1992
op het politieambt***Art. 52**

In hoofdstuk IV, afdeling 12, onderafdeling 8, van de wet van 5 augustus 1992 op het politieambt, ingevoegd bij de wet van 18 maart 2014 en laatste gewijzigd bij de wet van 31 juli 2020 wordt een artikel 44/11/9bis ingevoegd, luidende:

“Art. 44/11/9bis. Wanneer de leden van de politiediensten in het kader van hun opdrachten van bestuurlijke of gerechtelijke politie moeten samenwerken met de gezondheids-, hulp- en/of reddingsdiensten, kunnen zij persoonsgegevens en informatie meedelen voor zover deze toereikend, ter zake dienend en strikt noodzakelijk zijn om de leden van de gezondheids-, hulp- en/of reddingsdiensten in staat te stellen hun taken in optimale veiligheidsomstandigheden uit te voeren en om de veiligheid en de psychische en fysieke integriteit te waarborgen van eenieder bij de uitvoering van die taken.”

Afdeling 4*Wijzigingsbepalingen van de Consulaire Wetboek***Art. 53**

In artikel 39/4, derde lid, van de Consulaire Wetboek, ingevoegd bij de wet van 3 juli 2019, worden de woorden “het artikel 6, § 1, 1° of 1°/1, van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Terrorist Fighters” vervangen door de woorden “het artikel 2, 7° of 8°, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”) en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt”.

Art. 54

In artikel 65/1, derde lid, van dezelfde Wetboek, ingevoegd bij de wet van 3 juli 2019, worden de woorden “het artikel 6, § 1, 1° of 1°/1, van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Terrorist Fighters” vervangen door de

création de la banque de données commune “Terrorisme, Extrémisme, processus de Radicalisation” (“T.E.R.”) et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d’extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police”.

CHAPITRE 5

Dispositions abrogatoires

Art. 55

Dans la loi du 5 août 1992 sur la fonction de police, les articles suivants sont abrogés à la date d’entrée en vigueur de la présente loi:

1° l’article 44/2, paragraphe 2, inséré par la loi du 27 avril 2016;

2° l’article 44/4, paragraphe 2, alinéa 9, remplacé par la loi du 22 mai 2019;

3° la sous-section 7bis de la section 12 du chapitre IV, comportant les articles 44/11/3bis à 44/11/3quinquies/2, insérée par la loi du 27 avril 2016 et modifiée par la loi du 22 mai 2019.

Art. 56

Dans l’arrêté royal du 21 juillet 2016 relatif à la banque de données commune “Terrorist Fighters”, les articles suivants sont abrogés à la date d’entrée en vigueur de la présente loi:

1° l’article 1^{er}, 1°, 2°, 5°, et 7° à 17°, modifié par les arrêtés royaux des 23 avril 2018 et 20 décembre 2019;

2° l’article 2, modifié par les arrêtés royaux des 23 avril 2018 et 20 décembre 2019;

3° l’article 3, alinéa 1^{er}, 1^{er} tiret à 3^e tiret, modifié par les arrêtés royaux des 23 avril 2018 et 20 décembre 2019;

4° l’article 4, alinéa 1^{er}, 3^e et 4^e tirets;

5° l’article 5, modifié par les arrêtés royaux des 23 avril 2018 et 20 décembre 2019;

woorden “het artikel 2, 7° of 8°, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”) en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt”.

HOOFSTUK 5

Opheffingsbepalingen

Art. 55

In de wet van wet van 5 augustus 1992 op het politieambt, worden de volgende artikelen opgeheven op de datum van inwerkingtreding van deze wet:

1° artikel 44/2, paragraaf 2, ingevoegd bij de wet van 27 april 2016;

2° artikel 44/4, paragraaf 2, negende lid, vervangen door de wet van 22 mei 2019;

3° de onderafdeling 7bis van afdeling 12 van hoofdstuk IV, dat de artikelen 44/11/3bis tot 44/11/3quinquies/2 bevat, ingevoegd bij de wet van 27 april 2016 en gewijzigd bij de wet van 22 mei 2019.

Art. 56

In het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Terrorist Fighters, worden de volgende artikelen opgeheven op de datum van inwerkingtreding van deze wet:

1° artikel 1, 1°, 2°, 5°, en 7° tot 17°, gewijzigd bij de koninklijke besluiten van 23 april 2018 en 20 december 2019;

2° artikel 2, gewijzigd bij de koninklijke besluiten van 23 april 2018 en 20 december 2019;

3° artikel 3, eerste lid, eerste stripje tot derde stripje, gewijzigd bij de koninklijke besluiten van 23 april 2018 en 20 december 2019;

4° artikel 4, eerste lid, derde en vierde stripjes;

5° artikel 5, gewijzigd bij de koninklijke besluiten van 23 april 2018 en 20 december 2019;

6° l'article 6, modifié par les arrêtés royaux des 23 avril 2018 et 20 décembre 2019;

7° l'article 9, paragraphe 1^{er}, modifié par les arrêtés royaux des 23 avril 2018 et 20 décembre 2019;

8° l'article 10, remplacé par l'arrêté royal du 23 avril 2018;

9° les articles 11 à 15, modifiés par l'arrêté royal du 23 avril 2018;

10° l'article 16, modifié par les arrêtés royaux des 23 avril 2018 et 20 décembre 2019.

Art. 57

Dans l'arrêté royal du 23 avril 2018 relatif à la banque de données commune "Propagandistes de haine" et portant exécution de certaines dispositions de la section 1^{re}bis "de la gestion des informations" du chapitre IV de la loi sur la fonction de police, les articles suivants sont abrogés à la date d'entrée en vigueur de la présente loi:

1° l'article 1^{er}, 1°, 3°, 6°, et 8° à 15°, modifié par l'arrêté royal du 20 décembre 2019;

2° l'article 2;

3° l'article 3, alinéa 1^{er}, 1° à 3°, modifié par l'arrêté royal du 20 décembre 2019;

4° l'article 4, alinéa 1^{er}, 3° et 4°;

5° l'article 5, modifié par l'arrêté royal du 20 décembre 2019;

6° l'article 6;

7° l'article 9, paragraphe 1^{er};

8° les articles 10 à 16.

CHAPITRE 6

Dispositions finales

Art. 58

Le Roi peut remplacer les références existantes dans les lois et les arrêtés royaux aux dispositions de la loi sur la fonction de police par les références aux dispositions

6° artikel 6, gewijzigd bij de koninklijke besluiten van 23 april 2018 en 20 december 2019;

7° artikel 9, paragraaf 1, gewijzigd bij de koninklijke besluiten van 23 april 2018 en 20 december 2019;

8° artikel 10, vervangen door het koninklijk besluit van 23 april 2018;

9° artikelen 11 tot 15, gewijzigd bij het koninklijk besluit van 23 april 2018;

10° artikel 16, gewijzigd bij de koninklijke besluiten van 23 april 2018 en 20 december 2019.

Art. 57

In het koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1^{bis} "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt, worden de volgende artikelen opgeheven op de datum van inwerkingtreding van deze wet:

1° artikel 1, 1°, 3°, 6°, en 8° tot 15°, gewijzigd bij het koninklijk besluit van 20 december 2019;

2° artikel 2;

3° artikel 3, eerste lid, 1° tot 3°, gewijzigd bij het koninklijk besluit van 20 december 2019;

4° artikel 4, eerste lid, 3° en 4°;

5° artikel 5, gewijzigd bij het koninklijk besluit van 20 december 2019;

6° artikel 6;

7° artikel 9, paragraaf 1;

8° artikelen 10 tot 16.

CHAPITRE 6

Slotbepalingen

Art. 58

De Koning kan de bestaande verwijzingen in wetten en koninklijke besluiten naar bepalingen van de wet op het politieambt vervangen door verwijzingen naar de

correspondantes de la présente loi ou de ses arrêtés d'exécution.

Le Roi peut remplacer les références existantes dans les lois et les arrêtés royaux aux dispositions de l'arrêté royal du 21 juillet 2016 relatif à la banque de données commune "Terrorist Fighters" et de l'arrêté royal du 23 avril 2018 relatif à la banque de données commune "Propagandistes de haine" et portant exécution de certaines dispositions de la section 1re bis "de la gestion des informations" du chapitre IV de la loi sur la fonction de police, par les références aux dispositions correspondantes de la présente loi ou de ses arrêtés d'exécution.

Art. 59

Pour les entités enregistrées dans la banque de données commune visée à l'article 44/2, paragraphe 2, de la loi sur la fonction de police au moment de l'entrée en vigueur de la présente loi, la TFL procède à la concertation visée à l'article 33, § 1er, lorsque de nouvelles données à caractère personnel et informations visées à l'article 31 peuvent entraîner un changement de mesures à l'égard de l'entité concernée.

Art. 60

La présente loi entre en vigueur le 1er janvier 2025.

Le Roi peut fixer une date d'entrée en vigueur antérieure à celle mentionnée à l'alinéa 1er.

Donné à Bruxelles, le 20 novembre 2023

PHILIPPE

PAR LE ROI:

Le ministre de la Justice,

Paul Van Tigchelt

La ministre de l'Intérieur,

Annelies Verlinden

ermee overeenstemmende bepalingen van deze wet of van haar uitvoeringsbesluiten.

De Koning kan de bestaande verwijzingen in wetten en koninklijke besluiten naar bepalingen van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Terrorist Fighters en het koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1b/s "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt, vervangen door verwijzingen naar de ermee overeenstemmende bepalingen van deze wet of van haar uitvoeringsbesluiten.

Art. 59

De LTF gaat, voor de entiteiten die op het ogenblik van de inwerkingtreding van deze wet in de gemeenschappelijke gegevensbanken zoals bedoeld in artikel 44/2, paragraaf 2, van de wet op het politieambt zijn opgenomen, over tot het bij artikel 33, § 1, ingevoerd overleg wanneer nieuwe persoonsgegevens en informatie zoals bedoeld in artikel 31 kunnen leiden tot een verandering van maatregelen ten aanzien van de betrokken entiteit.

Art. 60

Deze wet treedt in werking op 1 januari 2025.

De Koning kan een datum van inwerkingtreding bepalen voorafgaand aan de datum vermeld in het eerste lid.

Gegeven te Brussel, 20 november 2023

FILIP

VAN KONINGSWEGE:

De minister van Justitie,

Paul Van Tigchelt

De minister van Binnenlandse Zaken,

Annelies Verlinden

Coordination des articles

TEXTE DE BASE

TEXTE ADAPTÉ AU PROJET DE LOI

Chapitre 4 – Dispositions modificatives

Section 1 - Dispositions modificatives de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

Art. 11.

§ 1^{er}. En application de l'article 23 du Règlement, les articles 12 à 22 et 34 du Règlement, ainsi que le principe de transparence du traitement visé à l'article 5 du Règlement, ne s'appliquent pas aux traitements de données à caractère personnel émanant directement ou indirectement des autorités visées au titre 3, à l'égard :

1° des autorités et personnes visées aux articles 14, 16 et 19 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité auxquelles ces données ont été transmises directement ou indirectement par les autorités visées au titre 3;

2° des autorités et personnes visées à l'article 2, alinéa 1^{er}, 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace ainsi que celles mentionnées à l'article 44/11/3^{ter} §§ 2 et 3, et à l'article 44/11/3^{quater} de la loi du 5 août 1992 sur la fonction de police, et qui relèvent du champ d'application du titre 1^{er}, et auxquelles ces données ont été transmises.

§ 2. Le responsable du traitement visé au présent titre qui est en possession de telles données ne les communique pas à la personne concernée à moins que :

Art. 11.

§ 1^{er}. En application de l'article 23 du Règlement, les articles 12 à 22 et 34 du Règlement, ainsi que le principe de transparence du traitement visé à l'article 5 du Règlement, ne s'appliquent pas aux traitements de données à caractère personnel émanant directement ou indirectement des autorités visées au titre 3, à l'égard :

1° des autorités et personnes visées aux articles 14, 16 et 19 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité auxquelles ces données ont été transmises directement ou indirectement par les autorités visées au titre 3;

2° des autorités et personnes visées à l'article 2, alinéa 1^{er}, 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace ainsi que celles mentionnées **aux articles 16 et 23, de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. ») et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police** et qui relèvent du champ d'application du titre 1^{er}, et auxquelles ces données ont été transmises.

§ 2. Le responsable du traitement visé au présent titre qui est en possession de telles données ne les communique pas à la personne concernée à moins que :

1° la loi l'y oblige dans le cadre d'une procédure contentieuse; ou

2° l'autorité visée au titre 3 concernée l'y autorise.

Le responsable du traitement ou l'autorité compétente ne fait aucune mention qu'il est en possession de données émanant des autorités visées au titre 3.

§ 3. Les limitations visées au paragraphe 1er portent également sur la journalisation des traitements d'une autorité visée au titre 3 dans les banques de données des responsables du traitement visés par le présent titre auxquelles l'autorité a directement accès.

§ 4. Le responsable de traitement visé au présent titre qui traite les données émanant directement ou indirectement des autorités visées au titre 3 répond au minimum aux conditions suivantes :

1° il adopte des mesures techniques ou organisationnelles appropriées pour assurer que l'accès aux données et les possibilités de traitement soient limités à ce dont les personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service;

2° il adopte des mesures techniques ou organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification ou tout autre traitement non autorisé de ces données.

Les membres du personnel du responsable de traitement qui traitent les données visées à l'alinéa 1er sont en outre tenus au devoir de discrétion.

§ 5. Lorsque l'autorité de contrôle visée dans la loi du 3 décembre 2017 portant création de l'Autorité de protection des données est saisie d'une requête ou d'une plainte où le responsable du traitement fait état de l'application du présent article, l'autorité de contrôle s'adresse au Comité permanent R pour qu'il fasse les vérifications

1° la loi l'y oblige dans le cadre d'une procédure contentieuse; ou

2° l'autorité visée au titre 3 concernée l'y autorise.

Le responsable du traitement ou l'autorité compétente ne fait aucune mention qu'il est en possession de données émanant des autorités visées au titre 3.

§ 3. Les limitations visées au paragraphe 1er portent également sur la journalisation des traitements d'une autorité visée au titre 3 dans les banques de données des responsables du traitement visés par le présent titre auxquelles l'autorité a directement accès.

§ 4. Le responsable de traitement visé au présent titre qui traite les données émanant directement ou indirectement des autorités visées au titre 3 répond au minimum aux conditions suivantes :

1° il adopte des mesures techniques ou organisationnelles appropriées pour assurer que l'accès aux données et les possibilités de traitement soient limités à ce dont les personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service;

2° il adopte des mesures techniques ou organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification ou tout autre traitement non autorisé de ces données.

Les membres du personnel du responsable de traitement qui traitent les données visées à l'alinéa 1er sont en outre tenus au devoir de discrétion.

§ 5. Lorsque l'autorité de contrôle visée dans la loi du 3 décembre 2017 portant création de l'Autorité de protection des données est saisie d'une requête ou d'une plainte où le responsable du traitement fait état de l'application du présent article, l'autorité de contrôle s'adresse au Comité permanent R pour qu'il fasse les vérifications

nécessaires auprès de l'autorité visée au titre 3.

Après réception de la réponse du Comité permanent R, l'Autorité de protection des données n'informe la personne concernée que des résultats de la vérification portant sur les données à caractère personnel n'émanant pas des autorités visées au titre 3 que l'autorité de contrôle est légalement tenue de communiquer.

Si la requête ou la plainte ne porte que sur des données à caractère personnel émanant d'une autorité visée au titre 3, l'Autorité de protection des données répond, après réception de la réponse du Comité permanent R, que les vérifications nécessaires ont été effectuées.

SOUS-TITRE 4. - De la protection des personnes physiques à l'égard du traitement des données à caractère personnel par l'organe de coordination pour l'analyse de la menace

Art. 138.

§ 1^{er}. Les définitions visées à l'article 26, 1° à 6°, 9°, 11° à 14° et 16° à 17°, s'appliquent au présent sous-titre.

§ 2. Pour l'application du présent sous-titre, on entend par :

1° "l'OCAM" : l'Organe de coordination pour l'analyse de la menace visé par la loi du 10 juillet 2006 relative à l'analyse de la menace;

2° "le responsable du traitement" : une personne physique ou morale, une autorité publique, un service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel;

3° "la loi du 18 juillet 1991" : la loi du 18 juillet 1991 organique du contrôle des

nécessaires auprès de l'autorité visée au titre 3.

Après réception de la réponse du Comité permanent R, l'Autorité de protection des données n'informe la personne concernée que des résultats de la vérification portant sur les données à caractère personnel n'émanant pas des autorités visées au titre 3 que l'autorité de contrôle est légalement tenue de communiquer.

Si la requête ou la plainte ne porte que sur des données à caractère personnel émanant d'une autorité visée au titre 3, l'Autorité de protection des données répond, après réception de la réponse du Comité permanent R, que les vérifications nécessaires ont été effectuées.

SOUS-TITRE 4. - De la protection des personnes physiques à l'égard du traitement des données à caractère personnel par l'organe de coordination pour l'analyse de la menace et dans la banque de données communes « Terrorisme, Extrémisme, processus de Radicalisation »

Art. 138.

§ 1^{er}. Les définitions visées à l'article 26, 1° à 6°, 9°, 11° à 14° et 16° à 17°, s'appliquent au présent sous-titre.

§ 2. Pour l'application du présent sous-titre, on entend par :

1° "l'OCAM" : l'Organe de coordination pour l'analyse de la menace visé par la loi du 10 juillet 2006 relative à l'analyse de la menace;

2° "le responsable du traitement" : une personne physique ou morale, une autorité publique, un service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel;

3° "la loi du 18 juillet 1991" : la loi du 18 juillet 1991 organique du contrôle des

services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace;

4° "la loi du 11 décembre 1998" : la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

5° "autorité de contrôle" : une autorité publique indépendante chargée par la loi de surveiller l'application de la présente loi;

6° "la loi du 10 juillet 2006" : la loi du 10 juillet 2006 relative à l'analyse de la menace;

7° "le système d'informations de l'OCAM" : le système d'informations visé à l'article 9 de la loi du 10 juillet 2006.

services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace;

4° "la loi du 11 décembre 1998" : la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

5° "autorité de contrôle" : une autorité publique indépendante chargée par la loi de surveiller l'application de la présente loi;

6° "la loi du 10 juillet 2006" : la loi du 10 juillet 2006 relative à l'analyse de la menace;

7° "le système d'informations de l'OCAM" : le système d'informations visé à l'article 9 de la loi du 10 juillet 2006.

8° « la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. ») » : la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. ») et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police ;

9° « la banque de données commune « T.E.R. » » : la banque de données visées à l'article 3 de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. ») ;

10° « les responsables conjoints du traitement de la banque de données commune « T.E.R. » » : les responsables du traitement visés à l'article 5, alinéa 1er, de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. »).

Art. 139

Le présent sous-titre s'applique à tout traitement de données à caractère personnel par l'OCAM et ses sous-traitants effectué dans le cadre des missions visées par la loi du 16 juillet 2006, ainsi que par ou en vertu de lois particulières.

Les titres 1er, 2, 4, 5, et 7 de la présente loi ne s'appliquent pas aux traitements visés à l'alinéa 1er. Dans le titre 6, seuls les articles 226, 227 et 230 s'appliquent.

Art. 139

Le présent sous-titre s'applique à tout traitement de données à caractère personnel par l'OCAM et ses sous-traitants effectué dans le cadre des missions visées par la loi du 16 juillet 2006, ainsi que par ou en vertu de lois particulières **et à tout traitement de données à caractère personnel dans la banque de données commune « T.E.R. ».**

Les titres 1er, 2, 4, 5, et 7 de la présente loi ne s'appliquent pas aux traitements visés à l'alinéa 1er. Dans le titre 6, seuls les articles 226, 227 et 230 s'appliquent.

Art. 140

Le traitement de données à caractère personnel ne peut être effectué que dans l'un des cas suivants :

1° lorsque la personne concernée a indubitablement donné son consentement;

2° lorsque le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée;

3° lorsque le traitement est utile au respect d'une obligation à laquelle l'OCAM est soumis par ou en vertu d'une loi;

4° lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou une autorité publique à laquelle les données à caractère personnel sont communiquées.

Art. 140

Le traitement de données à caractère personnel ne peut être effectué que dans l'un des cas suivants :

1° lorsque la personne concernée a indubitablement donné son consentement;

2° lorsque le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée;

3° lorsque le traitement est utile au respect d'une obligation à laquelle l'OCAM est soumis par ou en vertu d'une loi;

4° lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou une autorité publique à laquelle les données à caractère personnel sont communiquées.

5° lorsque le traitement est utile dans le cadre des finalités prévues à l'article 5, alinéa 2, de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme,

processus de Radicalisation» (« T.E.R. »).
».

Art. 143.

Les données à caractère personnel sont conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées et selon les modalités fixées dans l'article 9 de la loi du 16 juillet 2006 en ce qui concerne le système d'informations de l'OCAM et l'article 44/11/3bis de la loi de 5 août 1992 sur la fonction de police en ce qui concerne les banques de données communes dont l'OCAM est le gestionnaire opérationnel.

Art. 143.

Les données à caractère personnel sont conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées et selon les modalités fixées dans l'article 9 de la loi du 16 juillet 2006 en ce qui concerne le système d'informations de l'OCAM et **l'article 7 de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation» (« T.E.R. ») en ce qui concerne la banque de données commune « T.E.R. ».**

Art. 147

Les autorités de contrôle visées à l'article 161 et l'OCAM tiennent un journal des demandes d'exercice des droits par les personnes concernées.

Art. 147

Les autorités de contrôle visées à l'article 161, **les responsables conjoints du traitement de la banque de données commune « T.E.R. »** et l'OCAM tiennent un journal des demandes d'exercice des droits par les personnes concernées.

Art. 149

Le responsable du traitement :

1° fait toute diligence pour tenir les données à caractère personnel à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des dispositions du présent sous-titre;

2° veille à ce que, pour les personnes agissant sous son autorité, l'accès aux données à caractère personnel et les possibilités de traitement soient limités à ce qui est utile à l'exercice de leurs fonctions ou aux besoins de l'OCAM;

Art. 149

Le responsable du traitement :

1° fait toute diligence pour tenir les données à caractère personnel à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des dispositions du présent sous-titre;

2° veille à ce que, pour les personnes agissant sous son autorité, l'accès aux données à caractère personnel et les possibilités de traitement soient limités à ce qui est utile à l'exercice de leurs fonctions ou aux besoins de l'OCAM **ou dans le cadre des finalités de la banque de données**

3° informe les personnes agissant sous son autorité des dispositions du présent sous-titre et de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel.

commune « T.E.R. » visées à l'article 5, alinéa 2, de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. »);

3° informe les personnes agissant sous son autorité des dispositions du présent sous-titre et de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel.

Art. 155

§ 1^{er}. En cas de brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement concerné la notifie à l'autorité de contrôle compétente dans les meilleurs délais et si possible, 72 heures après en avoir pris connaissance.

§ 2. Le sous-traitant notifie au responsable du traitement toute brèche de sécurité dans les meilleurs délais.

§ 3. La notification visée aux paragraphes 1^{er} et 2 décrit ou communique, à tout le moins :

1° la nature de la brèche de sécurité y compris, si possible, le nombre estimé de personnes et d'enregistrements de données à caractère personnel concernés;

2° le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

3° les conséquences probables de la brèche de sécurité;

4° les mesures que le responsable du traitement ou le sous-traitant a prises ou propose de prendre pour remédier à la

Art. 155

§ 1^{er}. Sous réserve des dispositions de l'article 13 de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. »), en cas de brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement concerné la notifie à l'autorité de contrôle compétente dans les meilleurs délais et si possible, 72 heures après en avoir pris connaissance.

§ 2. Le sous-traitant notifie au responsable du traitement toute brèche de sécurité dans les meilleurs délais.

§ 3. La notification visée aux paragraphes 1^{er} et 2 décrit ou communique, à tout le moins :

1° la nature de la brèche de sécurité y compris, si possible, le nombre estimé de personnes et d'enregistrements de données à caractère personnel concernés;

2° le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

3° les conséquences probables de la brèche de sécurité;

4° les mesures que le responsable du traitement ou le sous-traitant a prises ou propose de prendre pour remédier à la

brèche de sécurité, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

brèche de sécurité, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Art. 156

§ 1^{er}. Le responsable du traitement tient un registre, classifié au sens de la loi du 11 décembre 1998, des banques de données de l'OCAM et de celles mises à sa disposition.

Ce registre comporte les informations suivantes :

1° pour les banques de données de l'OCAM :

a) les coordonnées du responsable du traitement et, le cas échéant, des responsables conjoints du traitement, et du délégué à la protection des données;

b) les finalités du traitement;

c) les catégories de destinataires auxquels des données à caractère personnel peuvent être communiquées;

d) dans la mesure du possible, les délais prévus pour l'effacement des données à caractère personnel;

e) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 154;

2° pour les banques de données mises à la disposition de l'OCAM :

a) les coordonnées du responsable du traitement et, si possible pour les pays hors de l'Union européenne le service gestionnaire de la banque de données et, le cas échéant, des responsables conjoints du traitement et du délégué à la protection des données;

Art. 156

§ 1^{er}. Le responsable du traitement tient un registre, classifié au sens de la loi du 11 décembre 1998, **de la banque de données commune « T.E.R. »**, des banques de données de l'OCAM et de celles mises à sa disposition.

Ce registre comporte les informations suivantes :

1° pour la banque de données commune « T.E.R. » et les banques de données de l'OCAM :

a) les coordonnées du responsable du traitement et, le cas échéant, des responsables conjoints du traitement, et du délégué à la protection des données;

b) les finalités du traitement;

c) les catégories de destinataires auxquels des données à caractère personnel peuvent être communiquées;

d) dans la mesure du possible, les délais prévus pour l'effacement des données à caractère personnel;

e) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 154;

2° pour les banques de données mises à la disposition de l'OCAM :

a) les coordonnées du responsable du traitement et, si possible pour les pays hors de l'Union européenne le service gestionnaire de la banque de données et, le cas échéant, des responsables conjoints du traitement et du délégué à la protection des données;

b) les finalités du traitement par l'OCAM.

§ 2. Chaque sous-traitant tient un registre, classifié au sens de la loi du 11 décembre 1998, de toutes les catégories d'activités de traitement effectuées pour le compte d'un responsable du traitement.

Ce registre comprend les éléments suivants :

1° les coordonnées du sous-traitant et du responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les coordonnées du délégué à la protection des données;

2° les catégories de traitements effectués pour le compte du responsable du traitement;

3° dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 154.

§ 3. Les registres visés aux paragraphes 1er et 2 se présentent sous une forme écrite y compris la forme électronique.

§ 4. Le responsable du traitement met le registre à la disposition de l'autorité de contrôle compétente à sa demande.

Le sous-traitant met le registre à la disposition du responsable du traitement ainsi qu'à la disposition de l'autorité de contrôle compétente à sa demande.

b) les finalités du traitement par l'OCAM.

§ 2. Chaque sous-traitant tient un registre, classifié au sens de la loi du 11 décembre 1998, de toutes les catégories d'activités de traitement effectuées pour le compte d'un responsable du traitement.

Ce registre comprend les éléments suivants :

1° les coordonnées du sous-traitant et du responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les coordonnées du délégué à la protection des données;

2° les catégories de traitements effectués pour le compte du responsable du traitement;

3° dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 154.

§ 3. Les registres visés aux paragraphes 1er et 2 se présentent sous une forme écrite y compris la forme électronique.

§ 4. Le responsable du traitement met le registre à la disposition de l'autorité de contrôle compétente à sa demande.

Le sous-traitant met le registre à la disposition du responsable du traitement ainsi qu'à la disposition de l'autorité de contrôle compétente à sa demande.

Art. 157/1 (nouveau)

§ 1er. Les responsables conjoints du traitement de la banque de données commune « T.E.R. » et, le cas échéant, le sous-traitant désignent un délégué à la protection des données. Cette décision est communiquée aux autorités de contrôle compétentes.

Le délégué à la protection des données est titulaire d'une habilitation de sécurité

de niveau « secret », au sens de la loi du 11 décembre 1998.

§ 2. Le délégué à la protection des données ne peut pas être sanctionné en raison de l'exercice de ses fonctions. Il ne peut pas non plus être relevé de ses fonctions en raison de l'exercice de ses missions, sauf s'il a commis une faute grave ou s'il ne remplit plus les conditions nécessaires à l'exercice de ses fonctions.

Le délégué à la protection des données peut s'adresser à l'Organe de contrôle de l'information policière ou au Comité permanent R pour contester cette décision.

§ 3. Il est chargé de manière indépendante :

1° de veiller au respect du présent sous-titre lors de tout traitement de données à caractère personnel dans le cadre de la banque de données commune « T.E.R. » ;

2° de conseiller toutes mesures utiles afin d'assurer la sécurité des données enregistrées dans la banque de données commune « T.E.R. » ;

3° d'informer et conseiller les responsables conjoints du traitement de la banque de données commune « T.E.R. », et le cas échéant, le gestionnaire, le responsable opérationnel, le sous-traitant, le dirigeant et le personnel du service concerné procédant au traitement sur les obligations qui leur incombent sur la base du présent sous-titre et de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. ») ;

4° de fournir des avis ou des recommandations aux responsables conjoints du traitement de la banque de données commune « T.E.R. », et le cas échéant, au gestionnaire, au responsable opérationnel et au sous-traitant ;

5° d'exécuter d'autres missions qui lui sont confiées par les responsables conjoints du traitement de la banque de données commune « T.E.R. », et le cas échéant, le responsable opérationnel ;

§4. Le délégué à la protection des données :

1° veille à la sensibilisation des utilisateurs dans les matières de protection des données à caractère personnel et de sécurité ;

2° coopère avec le gestionnaire dans le cadre de l'élaboration des procédures ;

3° coopère, si nécessaire avec les délégués à la protection des données des services qui traitent des données de la banque de données commune « T.E.R. » ;

4° est le point de contact avec les autorités de contrôle sur les questions relatives aux traitements réalisés dans la banque de données commune « T.E.R. ».

§ 5. Le délégué à la protection des données exerce ses fonctions en toute indépendance et dans le respect des compétences et missions respectives des services de base et des services partenaires.

Les responsables conjoints du traitement de la banque de données commune T.E.R., le gestionnaire et le responsable opérationnel veillent à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

Les responsables conjoints du traitement de la banque de données commune T.E.R. veillent à ce que le délégué à la protection des données dispose des ressources nécessaires pour exercer ses missions.

Le délégué à la protection des données peut être assisté par un ou plusieurs adjoints.

Il rend compte directement aux responsables conjoints du traitement de la banque de données commune T.E.R. qui en informent le responsable opérationnel.

§ 6. Le cas échéant, les modalités de fonctionnement, de désignation ainsi que les compétences requises du délégué à la protection des données peuvent être définies par le Roi.

Art. 158

Par dérogation aux articles 20, 22, 23, 58 et 59 de la présente loi et aux articles 35 et 36 du Règlement, un protocole, un avis du délégué à la protection des données, une analyse d'impact relative à la protection des données et l'avis résultant de la consultation de l'autorité de contrôle compétente ne peuvent pas être exigés comme condition préalable à la communication de données à caractère personnel entre l'OCAM et tout organisme public ou privé dans l'intérêt de l'exercice des missions de l'OCAM.

Cette communication se déroule conformément aux articles 8 à 12 de la loi du 10 juillet 2006 et au chapitre IV, section 12, sous-section 7bis, de la loi du 5 août 1992 sur la fonction de la police.

Par dérogation à l'article 20, § 1er, alinéa 2, lorsque les parties décident de conclure un protocole, celui-ci comprend :

1° l'identification de l'OCAM et de l'organisme public ou privé qui échangent les données à caractère personnel;

2° l'identification des responsables du traitement;

3° les coordonnées des délégués à la protection des données concernés;

Art. 158

Par dérogation aux articles 20, 22, 23, 58 et 59 de la présente loi et aux articles 35 et 36 du Règlement, un protocole, un avis du délégué à la protection des données, une analyse d'impact relative à la protection des données et l'avis résultant de la consultation de l'autorité de contrôle compétente ne peuvent pas être exigés comme condition préalable à la communication de données à caractère personnel entre l'OCAM et tout organisme public ou privé dans l'intérêt de l'exercice des missions de l'OCAM.

Par dérogation aux articles 20, 22, 23, 58 et 59 de la présente loi et aux articles 35 et 36 du Règlement, un protocole, un avis du délégué à la protection des données, une analyse d'impact relative à la protection des données et l'avis résultant de la consultation de l'autorité de contrôle compétente ne peuvent pas être exigés comme condition préalable à la communication de données à caractère personnel issues de la banque de données commune « T.E.R. » à tout organisme public ou privé dans l'intérêt de l'exercice des missions de prévention et de suivi du terrorisme et de l'extrémisme, lorsqu'il peut mener au terrorisme, visées à l'article 3, alinéa 1er, de la loi du [DATE] portant création de la banque de données commune «

4° les finalités pour lesquelles les données à caractère personnel sont transférées;

5° la base légale;

6° les restrictions aux droits de la personne concernée.

Le protocole visé à l'alinéa 3 porte le marquage "DIFFUSION RESTREINTE" au sens de l'arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998, pour autant qu'une classification au sens de la loi du 11 décembre 1998 ne se justifie pas.

Terrorisme, Extrémisme, processus de Radicalisation» (« T.E.R. »).

La communication visée à l'alinéa 1er se déroule conformément aux articles 8 à 12 de la loi du 10 juillet 2006

La communication visée à l'alinéa 2 se déroule conformément aux articles 20 à 28 de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation» (« T.E.R. »).

Par dérogation à l'article 20, § 1er, alinéa 2, lorsque les parties décident de conclure un protocole, celui-ci comprend :

1° l'identification de l'organisme public ou privé qui échangent les données à caractère personnel et, le cas échéant, l'identification de l'OCAM ;

2° l'identification des responsables du traitement;

3° les coordonnées des délégués à la protection des données concernés;

4° les finalités pour lesquelles les données à caractère personnel sont transférées;

5° la base légale;

6° les restrictions aux droits de la personne concernée.

Le protocole visé à l'alinéa 3 porte le marquage "DIFFUSION RESTREINTE" au sens de l'arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998, pour autant qu'une classification au sens de la loi du 11 décembre 1998 ne se justifie pas.

Art. 161

Le Comité permanent R, en sa qualité d'autorité publique indépendante, et le Comité permanent de Contrôle des Services de police, sont désignés comme autorités de

Art. 161.

Le Comité permanent R, en sa qualité d'autorité publique indépendante, et le Comité permanent de Contrôle des Services de police, sont désignés comme autorités de

protection des données chargée du contrôle du traitement des données à caractère personnel par l'OCAM et par ses sous-traitants selon les modalités fixées par la loi du 18 juillet 1991.

protection des données chargée du contrôle du traitement des données à caractère personnel par l'OCAM et par ses sous-traitants selon les modalités fixées par la loi du 18 juillet 1991.

Les autorités de contrôle visées à l'article 2, 22°, de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. ») sont désignées conjointement comme autorités de protection des données chargées du contrôle du traitement des données à caractère personnel dans la banque de données commune « T.E.R. ».

Art. 162

Par dérogation au titre 4, la consultation à des fins historiques, scientifiques ou statistiques des données à caractère personnel de l'OCAM et de son personnel par un responsable du traitement ultérieur est autorisée par l'OCAM si cela ne porte pas atteinte à ses missions visées dans la loi du 10 juillet 2006, à une information ou instruction judiciaire en cours ou aux relations que la Belgique entretient avec des Etats étrangers ou des organisations internationales et conformément à la loi du 10 juillet 2006.

Toute demande adressée aux Archives de l'Etat de traitement ultérieur de données à caractère personnel de l'OCAM et de son personnel à d'autres fins que celles visées à l'alinéa 1er est refusée à moins que la finalité soit légitime et que l'OCAM estime que le traitement n'est pas susceptible de porter atteinte aux intérêts visés à l'alinéa 1er.

Art. 162

Par dérogation au titre 4, la consultation à des fins historiques, scientifiques ou statistiques des données à caractère personnel de l'OCAM et de son personnel par un responsable du traitement ultérieur est autorisée par l'OCAM si cela ne porte pas atteinte à ses missions visées dans la loi du 10 juillet 2006, à une information ou instruction judiciaire en cours ou aux relations que la Belgique entretient avec des Etats étrangers ou des organisations internationales et conformément à la loi du 10 juillet 2006.

Toute demande adressée aux Archives de l'Etat de traitement ultérieur de données à caractère personnel de l'OCAM et de son personnel à d'autres fins que celles visées à l'alinéa 1er est refusée à moins que la finalité soit légitime et que l'OCAM estime que le traitement n'est pas susceptible de porter atteinte aux intérêts visés à l'alinéa 1er.

Par dérogation à l'alinéa 1er, la consultation à des fins historiques, scientifiques ou statistiques des données à caractère personnel relatives aux entités enregistrées dans la banque de données commune T.E.R. par un responsable du traitement ultérieur est autorisée par le responsable opérationnel de la banque de données commune « T.E.R. » après concertation avec les services de base visés à l'article

2, 2°, de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. »). Lorsqu'elle peut compromettre la sécurité d'une personne, l'exercice de l'action publique, l'exercice d'une enquête de renseignement ou la relation avec un service répressif d'un État étranger ou avec un service de renseignement et de sécurité d'un État étranger, la consultation est d'office refusée.

Toute demande adressée aux Archives de l'Etat de traitement ultérieur de données à caractère personnel enregistrées dans la banque de données commune T.E.R. à d'autres fins que celles visées à l'alinéa 1er est refusée à moins que la finalité soit légitime, qu'il n'y ait pas une atteinte disproportionnée à la vie privée et après avis du responsable opérationnel.

Art. 164

Les données à caractère personnel visées à l'article 162 sont rendues anonymes préalablement à leur consultation.

Si un traitement ultérieur de données anonymes ne permet pas d'atteindre les fins historiques, scientifiques ou statistiques, l'OCAM peut autoriser la consultation de données pseudonymisées.

Si l'anonymisation ou la pseudonymisation ne rend pas l'identification des données impossible, l'OCAM refuse la consultation si cela constitue une atteinte disproportionnée à la vie privée.

Art. 164

Les données à caractère personnel visées à l'article 162 sont rendues anonymes préalablement à leur consultation.

Si un traitement ultérieur de données anonymes ne permet pas d'atteindre les fins historiques, scientifiques ou statistiques, l'OCAM **ou le responsable opérationnel après concertation avec les services de base** visé à l'article 2, 2°, de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. ») pour ce qui concerne la banque de données commune T.E.R. peut autoriser la consultation de données pseudonymisées.

Si l'anonymisation ou la pseudonymisation ne rend pas l'identification des données impossible, l'OCAM **ou le responsable opérationnel après concertation avec les services de base** visé à l'article 2, 2°, de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. ») pour ce qui

concerne la banque de données commune T.E.R. refuse la consultation si cela constitue une atteinte disproportionnée à la vie privée.

Si un traitement ultérieur de données pseudonymisées ne permet pas d'atteindre les fins historiques, scientifiques ou statistiques, l'OCAM peut autoriser la consultation de données non pseudonymisées si cela ne porte pas une atteinte disproportionnée à la vie privée.

Si un traitement ultérieur de données pseudonymisées ne permet pas d'atteindre les fins historiques, scientifiques ou statistiques, l'OCAM **ou le responsable opérationnel après concertation avec les services de base visé à l'article 2, 2°, de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. »)** pour ce qui concerne la banque de données commune T.E.R. peut autoriser la consultation de données non pseudonymisées si cela ne porte pas une atteinte disproportionnée à la vie privée.

Art. 165

Par dérogation au titre 4, une communication ou publication des données à caractère personnel visées à l'article 162 non anonymisées ou non pseudonymisées, consultées par le responsable du traitement ultérieur n'est possible qu'avec l'accord de l'OCAM et sous les conditions que celui-ci aura fixées.

Art. 165

Par dérogation au titre 4, une communication ou publication des données à caractère personnel visées à l'article 162 non anonymisées ou non pseudonymisées, consultées par le responsable du traitement ultérieur n'est possible qu'avec l'accord de l'OCAM **ou du responsable opérationnel après concertation avec les services de base visé à l'article 2, 2°, de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. »)** pour ce qui concerne la banque de données commune T.E.R. et sous les conditions que celui-ci aura fixées.

Art. 166

Le responsable du traitement ultérieur des données à caractère personnel visées à l'article 162 tient un journal de ses activités de traitement ultérieur à des fins historiques, scientifiques ou statistiques.
Ce journal est classifié au sens de la loi du 11 décembre 1998 si le traitement porte sur des données classifiées.
Ce journal comporte les informations

Art. 166

Le responsable du traitement ultérieur des données à caractère personnel visées à l'article 162 tient un journal de ses activités de traitement ultérieur à des fins historiques, scientifiques ou statistiques.
Ce journal est classifié au sens de la loi du 11 décembre 1998 si le traitement porte sur des données classifiées.
Ce journal comporte les informations

suivantes	:	suivantes	:
1° les coordonnées du responsable du traitement initial, du responsable du traitement ultérieur et du délégué à la protection des données de ce dernier;		1° les coordonnées du responsable du traitement initial, du responsable du traitement ultérieur et du délégué à la protection des données de ce dernier;	
2° les finalités du traitement ultérieur;		2° les finalités du traitement ultérieur;	
3° les données faisant l'objet du traitement ultérieur;		3° les données faisant l'objet du traitement ultérieur;	
4° les éventuelles conditions du traitement ultérieur fixées par l'OCAM;		4° les éventuelles conditions du traitement ultérieur fixées par l'OCAM ou par le responsable opérationnel après concertation avec les services de base visé à l'article 2, 2°, de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. ») pour ce qui concerne la banque de données commune T.E.R.;	
5° les éventuels destinataires autorisés par l'OCAM.		5° les éventuels destinataires autorisés par l'OCAM ou par le responsable opérationnel après concertation avec les services de base visé à l'article 2, 2°, de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. ») pour ce qui concerne la banque de données commune T.E.R.	

Section 2 - Disposition modificative de la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme

Art. 4.

§ 1^{er}. Le chef de corps et/ou le représentant de la police locale qu'il désigne, visé à l'article 3, peut communiquer aux membres de la CSIL R les cartes d'information visées à l'article 1^{er}, 15°, de l'arrêté royal du 23 avril 2018 relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1^{er}bis "de la gestion des informations" du chapitre IV de la loi sur la fonction de police et à l'article 1^{er}, 12°, de l'arrêté royal du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters, des personnes dont le cas est soumis à la discussion en CSIL R conformément à l'article 3, § 2.

Art. 4.

§ 1^{er}. Le chef de corps et/ou le représentant de la police locale qu'il désigne, visé à l'article 3, peut communiquer aux membres de la CSIL R les cartes d'information visées à l'article 2, 17°, de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. ») et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police, des personnes dont le

cas est soumis à la discussion en CSIL R conformément à l'article 3, § 2.

§ 2. Le chef de corps et/ou le représentant de la police locale qu'il désigne, visé à l'article 3, peut, après approbation par consensus par tous les membres participant effectivement à la réunion de la CSIL R, communiquer une fiche de feed-back d'une personne dont le cas est soumis à la discussion en CSIL R, conformément à l'article 3, § 2, aux représentants des services visés à l'article 44/11/3ter, § 1er, de la loi du 5 août 1992 sur la fonction de police, compétents au sein de la zone géographique de la CSIL R concernée. La fiche de feed-back reprend une évaluation du suivi au sein de la CSIL R. La fiche de feed-back ne contient pas de secrets communiqués durant la concertation.

§ 2. Le chef de corps et/ou le représentant de la police locale qu'il désigne, visé à l'article 3, peut, après approbation par consensus par tous les membres participant effectivement à la réunion de la CSIL R, communiquer une fiche de feed-back d'une personne dont le cas est soumis à la discussion en CSIL R, conformément à l'article 3, § 2, aux représentants des services visés à l'article 2, 2° et 22°, de la loi du [DATE] portant création de la banque de données commune « **Terrorisme, Extrémisme, processus de Radicalisation** » (« T.E.R. ») et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police, compétents au sein de la zone géographique de la CSIL R concernée. La fiche de feed-back reprend une évaluation du suivi au sein de la CSIL R. La fiche de feed-back ne contient pas de secrets communiqués durant la concertation.

§ 3. Le traitement des données à caractère personnel relatives aux personnes soumises à la discussion en CSIL R, conformément à l'article 3, § 2, n'est pas autorisé, sous réserve des exceptions prévues par la loi.

§ 3. Le traitement des données à caractère personnel relatives aux personnes soumises à la discussion en CSIL R, conformément à l'article 3, § 2, n'est pas autorisé, sous réserve des exceptions prévues par la loi.

Section 3 - Dispositions modificatives de la loi du 5 août 1992 sur la fonction de police

Art. 44/2.

§ 1^{er}. Lorsque l'exercice des missions de police administrative et de police judiciaire nécessite que les services de police structurent les données à caractère personnel et les informations visées à l'article 44/1 de sorte qu'elles puissent être directement retrouvées, celles-ci sont traitées dans une banque de données policière opérationnelle, appartenant à l'une

Art. 44/2.

§ 1^{er}. Lorsque l'exercice des missions de police administrative et de police judiciaire nécessite que les services de police structurent les données à caractère personnel et les informations visées à l'article 44/1 de sorte qu'elles puissent être directement retrouvées, celles-ci sont traitées dans une banque de données policière opérationnelle, appartenant à l'une

des catégories de banques de données visées à l'alinéa 2 selon les finalités propres à chaque catégorie de banques de données.

Les catégories de banques de données policières opérationnelles sont les suivantes :

1° la Banque de données Nationale Générale, ci-après dénommée "B.N.G.";

2° les banques de données de base;

3° les banques de données particulières.

Les finalités visées à l'alinéa 1er sont spécifiées respectivement dans les articles 44/7, 44/11/2, § 1er et 44/11/3, § 2.

§ 2. Lorsque l'exercice conjoint, par tout ou partie des autorités, organes, organismes, services, directions ou commission visés à l'article 44/11/3ter, chacun dans le cadre de ses compétences légales, des missions de prévention et de suivi du terrorisme au sens de l'article 8, 1°, b) de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ou de l'extrémisme au sens de l'article 8, 1° c) de la même loi, lorsqu'il peut mener au terrorisme, nécessite que ceux-ci structurent les données à caractère personnel et les informations relatives à ces missions de sorte qu'elles puissent être directement retrouvées, ces données à caractère personnel et ces informations sont traitées dans une ou plusieurs banques de données communes.

Les conditions de création des banques de données communes et de traitement de données à caractère personnel et des informations dans ces banques de données sont spécifiées à l'article 44/11/3bis.

L'article 139, alinéa 2, du Code pénal s'applique aux banques de données communes.

§ 3. Lorsque dans le cadre de l'exercice des missions de police administrative et judiciaire, des outils techniques sont utilisés pour collecter de manière automatique des données à caractère personnel et des informations de nature technique,

des catégories de banques de données visées à l'alinéa 2 selon les finalités propres à chaque catégorie de banques de données.

Les catégories de banques de données policières opérationnelles sont les suivantes :

1° la Banque de données Nationale Générale, ci-après dénommée "B.N.G.";

2° les banques de données de base;

3° les banques de données particulières.

Les finalités visées à l'alinéa 1er sont spécifiées respectivement dans les articles 44/7, 44/11/2, § 1er et 44/11/3, § 2.

§2. [...]

§ 3. Lorsque dans le cadre de l'exercice des missions de police administrative et judiciaire, des outils techniques sont utilisés pour collecter de manière automatique des données à caractère personnel et des informations de nature technique, structurées de sorte qu'elles puissent être

structurées de sorte qu'elles puissent être directement retrouvées, ces données sont traitées dans une banque de données technique.

Une banque de données technique est créée suite à l'utilisation de :

1° caméras intelligentes de reconnaissance automatique de plaques d'immatriculation;

2° systèmes intelligents de reconnaissance automatique de plaques d'immatriculation.

Par systèmes intelligents de reconnaissance automatique de plaques d'immatriculation, l'on entend tout logiciel informatique intelligent permettant de traiter automatiquement les images enregistrées au moyen de caméras, pour en extraire les données de plaques d'immatriculation, sur la base de certains critères préétablis.

Une banque de données technique peut être créée tant au niveau local qu'au niveau national.

Les conditions de création de ce type de banques de données et les conditions de traitement des données à caractère personnel et informations qui y figurent sont spécifiées aux articles 44/11/3sexies à 44/11/3decies.

Art. 44/4.

§ 1^{er}. En matière de police administrative, le responsable du traitement des données à caractère personnel et des informations visées à l'article 44/1, y compris celles incluses dans les banques de données visées à l'article 44/2, § 1^{er}, alinéa 2, 1° et 2°, est le ministre de l'Intérieur.

En matière de police judiciaire, le responsable du traitement des données à caractère personnel et des informations visées à l'article 44/1, y compris celles incluses dans les banques de données visées à l'article 44/2, § 1^{er}, alinéa 2, 1° et 2°, est le ministre de la Justice.

directement retrouvées, ces données sont traitées dans une banque de données technique.

Une banque de données technique est créée suite à l'utilisation de :

1° caméras intelligentes de reconnaissance automatique de plaques d'immatriculation;

2° systèmes intelligents de reconnaissance automatique de plaques d'immatriculation.

Par systèmes intelligents de reconnaissance automatique de plaques d'immatriculation, l'on entend tout logiciel informatique intelligent permettant de traiter automatiquement les images enregistrées au moyen de caméras, pour en extraire les données de plaques d'immatriculation, sur la base de certains critères préétablis.

Une banque de données technique peut être créée tant au niveau local qu'au niveau national.

Les conditions de création de ce type de banques de données et les conditions de traitement des données à caractère personnel et informations qui y figurent sont spécifiées aux articles 44/11/3sexies à 44/11/3decies.

Art. 44/4.

§ 1^{er}. En matière de police administrative, le responsable du traitement des données à caractère personnel et des informations visées à l'article 44/1, y compris celles incluses dans les banques de données visées à l'article 44/2, § 1^{er}, alinéa 2, 1° et 2°, est le ministre de l'Intérieur.

En matière de police judiciaire, le responsable du traitement des données à caractère personnel et des informations visées à l'article 44/1, y compris celles incluses dans les banques de données visées à l'article 44/2, § 1^{er}, alinéa 2, 1° et 2°, est le ministre de la Justice.

Pour ce qui concerne les banques de données visées à l'article 44/2, § 1er, alinéa 2, 3°, les chefs de corps, le commissaire général, les directeurs généraux ou les directeurs qui ont fixé les objectifs et les moyens relatifs à ces banques de données particulières sont les responsables du traitement.

§ 2. Les ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences et sans préjudice des compétences propres des autorités judiciaires, déterminent par directives contraignantes les mesures nécessaires en vue d'assurer la gestion et la sécurité dont notamment les aspects relatifs à la fiabilité, la confidentialité, la disponibilité, la traçabilité et l'intégrité des données à caractère personnel et des informations traitées dans les banques de données visées à l'article 44/2.

Les fichiers de journalisation sont établis dans les banques de données visées à l'article 44/2 au moins pour les traitements suivants: la collecte, la modification, la consultation, la communication, y compris les transferts, l'archivage, l'interconnexion et l'effacement.

Les fichiers de journalisation de consultation et de communication permettent d'établir:

1° le motif, la date et l'heure de ces traitements;

2° les catégories de personnes qui ont consulté les données à caractère personnel, ainsi que l'identification de la personne qui a consulté ces données;

3° les systèmes qui ont communiqué ces données;

4° les catégories de destinataires des données à caractère personnel, et si possible, l'identité des destinataires de ces données.

Le Roi peut déterminer, par arrêté délibéré en Conseil des ministres après avis de l'Organe de contrôle, d'autres types de

Pour ce qui concerne les banques de données visées à l'article 44/2, § 1er, alinéa 2, 3°, les chefs de corps, le commissaire général, les directeurs généraux ou les directeurs qui ont fixé les objectifs et les moyens relatifs à ces banques de données particulières sont les responsables du traitement.

§ 2. Les ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences et sans préjudice des compétences propres des autorités judiciaires, déterminent par directives contraignantes les mesures nécessaires en vue d'assurer la gestion et la sécurité dont notamment les aspects relatifs à la fiabilité, la confidentialité, la disponibilité, la traçabilité et l'intégrité des données à caractère personnel et des informations traitées dans les banques de données visées à l'article 44/2.

Les fichiers de journalisation sont établis dans les banques de données visées à l'article 44/2 au moins pour les traitements suivants: la collecte, la modification, la consultation, la communication, y compris les transferts, l'archivage, l'interconnexion et l'effacement.

Les fichiers de journalisation de consultation et de communication permettent d'établir:

1° le motif, la date et l'heure de ces traitements;

2° les catégories de personnes qui ont consulté les données à caractère personnel, ainsi que l'identification de la personne qui a consulté ces données;

3° les systèmes qui ont communiqué ces données;

4° les catégories de destinataires des données à caractère personnel, et si possible, l'identité des destinataires de ces données.

Le Roi peut déterminer, par arrêté délibéré en Conseil des ministres après avis de l'Organe de contrôle, d'autres types de

traitements pour lesquels les fichiers de journalisation sont établis.

Des mesures appropriées sont adoptées pour assurer la sécurité des fichiers de journalisation et, en particulier, pour empêcher tout traitement non autorisé et pour assurer l'intégrité des données traitées.

Les procédures d'accès aux fichiers de journalisation garantissent la nécessité et la proportionnalité de l'accès aux données de journalisation en vue d'atteindre les finalités visées à l'article 56, § 2, de la loi relative à la protection des données.

Ces procédures sont soumises à l'avis de l'Organe de contrôle.

Les chefs de corps pour la police locale et le commissaire général, les directeurs généraux et les directeurs pour la police fédérale sont les garants de la bonne exécution de ces directives en ce qui concerne les banques de données visées à l'article 44/2, §§ 1^{er}, et 3.

Le gestionnaire, désigné en droit ou dans les faits est le garant de la bonne exécution de ces directives en ce qui concerne les banques de données visées à l'article 44/2, § 2.

§ 3. Sans préjudice des compétences des autorités judiciaires, les ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences, déterminent par directive générale et contraignante, publiée au Moniteur belge, les règles d'accès des membres des services de police aux banques de données visées à l'article 44/2, §§ 1^{er}, et 3.

§ 4. Les ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences, déterminent par directive générale et contraignante publiée au Moniteur belge, les modalités relatives à l'interconnexion des banques de données visées à l'article 44/2 entre elles ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique.

traitements pour lesquels les fichiers de journalisation sont établis.

Des mesures appropriées sont adoptées pour assurer la sécurité des fichiers de journalisation et, en particulier, pour empêcher tout traitement non autorisé et pour assurer l'intégrité des données traitées.

Les procédures d'accès aux fichiers de journalisation garantissent la nécessité et la proportionnalité de l'accès aux données de journalisation en vue d'atteindre les finalités visées à l'article 56, § 2, de la loi relative à la protection des données.

Ces procédures sont soumises à l'avis de l'Organe de contrôle.

Les chefs de corps pour la police locale et le commissaire général, les directeurs généraux et les directeurs pour la police fédérale sont les garants de la bonne exécution de ces directives en ce qui concerne les banques de données visées à l'article 44/2, §§ 1^{er}, et 3.

[...]

§ 3. Sans préjudice des compétences des autorités judiciaires, les ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences, déterminent par directive générale et contraignante, publiée au Moniteur belge, les règles d'accès des membres des services de police aux banques de données visées à l'article 44/2, §§ 1^{er}, et 3.

§ 4. Les ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences, déterminent par directive générale et contraignante publiée au Moniteur belge, les modalités relatives à l'interconnexion des banques de données visées à l'article 44/2 entre elles ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique.

Ces directives déterminent au moins, sur la base du caractère pertinent, adéquat et non excessif, les catégories de banques de données qui peuvent être connectées entre elles, les modalités relatives à l'interconnexion et les règles d'accès des membres des services de police relatives à l'existence d'une information pertinente au sein de ces banques de données interconnectées ou, le cas échéant, aux données elles-mêmes ainsi qu'aux traitements qui en résultent.

§ 5. Les profils et les modalités d'accès visés aux §§ 3 et 4 sont déterminés notamment sur la base:

1° du besoin d'en connaître, en ce compris de la nécessité de croiser ou coordonner les données traitées;

2° des finalités légales de chaque banque de données;

3° des différentes catégories de personnes visées à l'article 44/5;

4° de l'évaluation des données;

5° de l'état de validation des données traitées.

Les accès visés aux §§ 3 et 4 doivent être conçus à la base ou par défaut de telle sorte que les données évaluées et validées apparaissent de manière claire et puissent être exploitées prioritairement.

Les profils d'accès et l'identification des personnes ayant accès sont tenus à la disposition de l'Organe de contrôle.

§ 6. Les ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences, déterminent par directive générale et contraignante publiée au Moniteur belge les mesures adéquates, pertinentes et non excessives relatives à l'interconnexion ou la corrélation des banques de données techniques visées à l'article 44/2, § 3, avec les banques de données visées à l'article 44/2, §§ 1er et 2, ou avec d'autres banques de données auxquelles les services de police ont accès

Ces directives déterminent au moins, sur la base du caractère pertinent, adéquat et non excessif, les catégories de banques de données qui peuvent être connectées entre elles, les modalités relatives à l'interconnexion et les règles d'accès des membres des services de police relatives à l'existence d'une information pertinente au sein de ces banques de données interconnectées ou, le cas échéant, aux données elles-mêmes ainsi qu'aux traitements qui en résultent.

§ 5. Les profils et les modalités d'accès visés aux §§ 3 et 4 sont déterminés notamment sur la base:

1° du besoin d'en connaître, en ce compris de la nécessité de croiser ou coordonner les données traitées;

2° des finalités légales de chaque banque de données;

3° des différentes catégories de personnes visées à l'article 44/5;

4° de l'évaluation des données;

5° de l'état de validation des données traitées.

Les accès visés aux §§ 3 et 4 doivent être conçus à la base ou par défaut de telle sorte que les données évaluées et validées apparaissent de manière claire et puissent être exploitées prioritairement.

Les profils d'accès et l'identification des personnes ayant accès sont tenus à la disposition de l'Organe de contrôle.

§ 6. Les ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences, déterminent par directive générale et contraignante publiée au Moniteur belge les mesures adéquates, pertinentes et non excessives relatives à l'interconnexion ou la corrélation des banques de données techniques visées à l'article 44/2, § 3, avec les banques de données visées à l'article 44/2, §§ 1er et 2, ou avec d'autres banques de données auxquelles les services de police ont accès

par ou en vertu de la loi ou de traités internationaux liant la Belgique.

Cette directive tient compte des critères de temps, d'espace et de fréquence des interconnexions et corrélations. Elles déterminent au moins l'autorité qui permet ce genre de mesures, ainsi que les banques de données qui peuvent être connectées entre elles

Sous-section 7bis. - Des banques de données communes.

Art. 44/11/3bis.

§ 1^{er}. Pour l'exercice conjoint des missions visées à l'article 44/2, § 2, les ministres de l'Intérieur et de la Justice peuvent conjointement créer des banques de données communes dont ils deviennent responsables du traitement.

§ 2. La création d'une banque de données commune est motivée par une des finalités suivantes :

1° la nécessité stratégique, tactique ou opérationnelle de traiter en commun des données à caractère personnel et des informations pour exercer les missions respectives des autorités, organes, organismes, services, directions ou commission visées à l'article 44/2, § 2;

2° l'aide à la prise de décisions par les autorités administratives, de police administrative ou de police judiciaire.

§ 3. Préalablement à sa création, les ministres de l'Intérieur et de la Justice déclarent la banque de données commune, ainsi que les modalités de traitement, dont celles relatives à l'enregistrement des données, et les différentes catégories et types de données à caractère personnel et d'informations traitées, aux Comité et l'Organe de contrôle visés à l'article 44/11/3quinquies/2, qui émettent

par ou en vertu de la loi ou de traités internationaux liant la Belgique.

Cette directive tient compte des critères de temps, d'espace et de fréquence des interconnexions et corrélations. Elles déterminent au moins l'autorité qui permet ce genre de mesures, ainsi que les banques de données qui peuvent être connectées entre elles

Sous-section 7bis. - Des banques de données communes.

Abrogée

Art. 44/11/3bis.

Abrogé

conjointement un avis dans les 30 jours à partir de la réception de la déclaration.

§ 4. Les banques de données communes permettent le traitement de différentes catégories de données à caractère personnel relatives notamment aux personnes, aux groupements, aux organisations et aux phénomènes qui sont adéquates, pertinentes et non excessives au regard des missions visées à l'article 44/2, § 2, et des finalités visées au § 2.

Pour chaque banque de données commune, un arrêté royal délibéré en Conseil des ministres détermine, après avis du Comité et de l'Organe de contrôle visés à l'article 44/11/3^{quinquies}/2, les types de données à caractère personnel traitées, les règles de responsabilités en matière de protection des données à caractère personnel des organes, services, autorités et organismes traitant des données, les règles en matière de sécurité des traitements, les règles d'utilisation, de conservation et d'effacement des données.

§ 5. Les données à caractère personnel conservées au sein des banques de données communes sont supprimées dès que les finalités visées au § 2 disparaissent, et au maximum 30 ans après le dernier traitement, sans préjudice de la loi du 24 juin 1955 relative aux archives.

Après le dernier traitement, il est examiné au minimum tous les trois ans si les données à caractère personnel présentent toujours un lien direct avec l'une des finalités du § 2. Si tel n'est pas le cas, les données sont supprimées.

§ 6. Tous les traitements réalisés par les directions, services, organes, organismes, autorités ou commission, dans les banques de données communes font l'objet d'une journalisation qui est conservée pendant 30 ans à partir du traitement réalisé dans les banques de données communes.

§ 7. Les données à caractère personnel et les informations qui doivent être supprimées peuvent être archivées pour une durée de maximum 30 ans.

À l'issue de ce délai, ces données et informations sont effacées, sans préjudice de la loi du 24 juin 1955 relative aux archives.

La consultation des archives d'une banque de données communes ne peut être réalisée que dans le cadre des finalités suivantes :

1° l'appui à la définition et à la réalisation de la politique policière et de sécurité en matière de terrorisme et d'extrémisme pouvant mener au terrorisme;

2° le traitement des antécédents dans le cadre d'une enquête relative à un fait criminel de terrorisme;

3° la défense des autorités visées à l'article 44/11/3bis § 2, 2° en justice.

Le résultat de l'exploitation des archives de la banque de données commune pour la finalité prévue à l'alinéa 1^{er}, 1°, est anonymisé.

§ 8. Des modalités complémentaires de gestion des banques de données communes peuvent être déterminées par un arrêté royal délibéré en Conseil des ministres, après avis du Comité et de l'Organe de contrôle visés à l'article 44/11/3quinquies/2.

§ 9. Un gestionnaire est désigné pour chaque banque de données commune, par le Roi, sur proposition conjointe des ministres de l'Intérieur et de la Justice. Ce gestionnaire est chargé de la gestion technique et fonctionnelle de la banque de données commune.

Le gestionnaire assure au moins les missions suivantes :

- créer et mettre à la disposition la banque de données commune en recourant aux moyens techniques nécessaires sur la base des possibilités découlant de l'environnement ICT propre à son service;

- gérer la banque de données commune et en assurer sa maintenance;

- traduire en règles fonctionnelles les modalités relatives au traitement de l'information déclarées par les ministres en vertu du § 3;

- déterminer et faire appliquer les normes techniques nécessaires au fonctionnement de la banque de données commune;

- fournir un avis sur le plan technique et/ou fonctionnel à la demande du responsable opérationnel ou du délégué à la protection des données visé à l'article 44/11/3quinquies/1;

- organiser les droits et les accès nécessaires aux traitements à effectuer dans la banque de données commune;

- fournir une documentation et une assistance technique;

- gérer et traiter les rapportages des incidents de sécurité tant sur le plan technique que fonctionnel.

§ 10. Un responsable opérationnel est désigné pour chaque banque de données commune, par le Roi, sur proposition conjointe des ministres de l'Intérieur et de la Justice. Ce responsable est chargé de la gestion opérationnelle de la banque de données commune.

Le responsable opérationnel assure au moins les missions suivantes :

- contrôler la qualité des données traitées au sein de la banque de données commune et s'assurer de leur pertinence au regard des finalités pour lesquelles la banque de données a été créée;

- exercer une fonction de coordination pour l'alimentation de la banque de données commune par les différents services;

- organiser la collaboration adéquate entre les services partenaires en vue de réaliser les finalités prévues;

- veiller à ce que l'exploitation des données à caractère personnel et des informations réponde aux finalités décrites au § 2.

§ 11. Pour chaque banque de données commune, des missions spécifiques du gestionnaire et du responsable opérationnel peuvent être déterminées par le Roi.

Art. 44/11/3ter.

§ 1^{er}. Sur la base du besoin d'en connaître, tout ou partie des données à caractère personnel et des informations des banques de données communes sont directement accessibles à l'Organe et aux services suivants, chargés de compétences dans les domaines visés à l'article 44/2, § 2 :

- a) l'Organe pour la coordination de l'analyse de la menace;
- b) la police intégrée;
- c) les services de renseignement et de sécurité.

Dans le cadre de l'exercice de leurs missions visées à l'article 44/11/3quinquies/2, tout ou partie des données à caractère personnel et des informations des banques de données communes sont directement accessibles au Comité et à l'Organe de contrôle visés à l'article 44/11/3quinquies/2.

§ 2. Sur la base du besoin d'en connaître, notamment au niveau stratégique, tactique ou opérationnel, les données à caractère personnel et les informations des banques de données communes peuvent être communiquées ou être directement accessibles aux services suivants ou faire l'objet d'une interrogation directe par ces services, lorsqu'ils sont chargés de compétences dans les domaines prévus à l'article 44/2, § 2 :

- a) la Commission permanente de la police locale;
- b) la Direction générale Centre de crise;
- c) la Direction générale Sécurité et Prévention du service Public Fédéral Intérieur;

Art. 44/11/3ter.

Abrogé

d) la Direction générale des Etablissements pénitentiaires et les établissements pénitentiaires;

e) le Service Public Fédéral Affaires étrangères, Direction générale Affaires consulaires;

f) le Ministère public;

g) la Cellule de traitement des informations financières;

h) l'Office des Etrangers;

i) les services d'enquête et recherche de l'Administration générale des douanes et accises.

Par arrêté délibéré en Conseil des ministres, après avis du Comité et de l'Organe de contrôle visés à l'article 44/11/3*quinquies*/2, le Roi détermine le type d'accès et ses modalités pour les organes, autorités, directions ou services visés à l'alinéa 1^{er}.

§ 3. Par arrêté délibéré en Conseil des ministres, après avis du Comité et de l'Organe de contrôle visés à l'article 44/11/3*quinquies*/2, le Roi peut déterminer d'autres autorités publiques belges, organes ou organismes publics ou d'intérêt public chargés par la loi de l'application de la loi pénale ou qui ont des missions légales de sécurité publique, qui, lorsqu'ils sont chargés de compétences dans les domaines prévus à l'article 44/2, § 2, peuvent accéder, sur la base du besoin d'en connaître, notamment au niveau stratégique, tactique ou opérationnel aux banques de données communes.

Par arrêté délibéré en Conseil des ministres, après avis du Comité et de l'Organe de contrôle visés à l'article 44/11/3*quinquies*/2, le Roi détermine le type d'accès et ses modalités pour les organes, autorités, directions ou services visés à l'alinéa 1^{er}.

En outre, sur base du besoin d'en connaître, notamment au niveau stratégique, tactique ou opérationnel, les

ministres de l'Intérieur et de la Justice désignent conjointement les organes, autorités ou organismes prévus à l'alinéa 1er auxquels les données à caractère personnel et informations extraites des banques de données communes peuvent être communiquées.

Ces organes, autorités ou organismes sont déterminés dans la déclaration préalable visée à l'article 44/11/3*bis*, § 3.

§ 4. L'Organe et les services visés au § 1^{er} ainsi que les directions, services, organes, organismes, autorités ou commission visés aux §§ 2 et 3 qui accèdent directement aux banques de données communes transmettent d'office aux banques de données communes les données à caractère personnel et les informations visées à l'article 44/2, § 2. Ces données à caractère personnel et informations sont enregistrées dans les banques de données communes, sous leur responsabilité et suivant leurs procédures internes de validation, conformément aux règles qui sont déterminées par le Roi après avoir recueilli l'avis visé à l'article 44/11/3*bis*, § 3.

Les données à caractère personnel et les informations introduites dans les banques de données communes sont immédiatement communiquées au chef de corps de chaque zone de police concernée. Dans le respect des conditions prévues à l'article 44/1, § 4, et en application de cet article, celui-ci informe les autorités de police administrative compétentes.

§ 5. Par dérogation au § 4, l'obligation d'alimenter les banques de données communes est différée lorsque et aussi longtemps que le magistrat compétent, avec l'accord du procureur fédéral, estime que cette alimentation peut compromettre l'exercice de l'action publique ou la sécurité d'une personne. Le cas échéant, le procureur fédéral peut déterminer les modalités de cette dérogation. Le procureur fédéral vérifie, à échéances régulières, la nécessité du maintien de l'ajournement de l'alimentation des banques de données communes.

Par dérogation au § 4, l'obligation d'alimenter les banques de données communes est différée, lorsque et aussi longtemps que le dirigeant d'un service du renseignement et de sécurité estime que cette alimentation peut compromettre la sécurité d'une personne ou lorsque l'information émane d'un service étranger qui a explicitement demandé de ne pas le transmettre à d'autres services.

Art. 44/11/3^{quater}.

Aux fins de renforcer la prévention et la lutte contre le terrorisme et l'extrémisme pouvant mener au terrorisme, les données à caractère personnel et informations extraites d'une banque de données communes peuvent être communiquées selon les modalités déterminées par le Roi, à une autorité ou une entité tierce après évaluation par le gestionnaire, le responsable opérationnel, l'Organe et les services visés à l'article 44/11/3^{ter}, § 1^{er}.

Abrogé

Art. 44/11/3^{quater}.

Art. 44/11/3^{quinquies}.

Pour les finalités visées à l'article 44/2, § 2, sans préjudice des règles internationales liant la Belgique, les données à caractère personnel et les informations des banques de données communes peuvent être communiquées aux services de police étrangers, aux organisations internationales de coopération judiciaire et policière et aux services de répression internationaux conformément à l'article 44/11/13.

Abrogé

Art. 44/11/3^{quinquies}.

Pour les finalités visées à l'article 44/2, § 2, sans préjudice des règles internationales liant la Belgique, les données à caractère personnel et les informations des banques de données communes peuvent être communiquées aux services de renseignement étrangers et aux organes étrangers chargés de l'analyse de la menace ou équivalents conformément aux articles 21 et 22 de la loi du 8 décembre 1992 relative à la protection de la vie privée à

l'égard des traitements de données à caractère personnel.

Le Roi détermine les modalités de la communication visée aux alinéas 1^{er} et 2.

Art. 44/11/3quinquies/1.

Un délégué à la protection des données est désigné conjointement par les ministres de l'Intérieur et de la Justice pour les données à caractère personnel et informations traitées dans le cadre des banques de données communes visées à l'article 44/2, § 2.

En complément des missions prévues dans la loi relative à la protection des données, le délégué à la protection des données est chargé:

1° de la fourniture d'avis qualifiés en matière de protection des données et de sécurisation des données à caractère personnel et informations et de leur traitement et, plus particulièrement, il veille au respect des conditions générales de licéité du traitement à l'égard des traitements de données à caractère personnel;

2° de la mise en oeuvre, de la mise à jour et du contrôle d'une politique de sécurisation et de protection des données;

3° de l'exécution des autres missions relatives à la protection des données et à la sécurisation qui sont déterminées par le Roi ou qui lui sont confiées par les ministres de l'Intérieur et de la Justice.

Il exerce ses fonctions en toute indépendance par rapport aux autorités, organes, organismes, services et directions visés à l'article 44/11/3^{ter}. Il rend compte directement aux ministres de l'Intérieur et de la Justice.

Art. 44/11/3quinquies/2.

Dans le respect de l'exercice de leurs missions respectives, le contrôle du

Art. 44/11/3quinquies/1.

Abrogé

Art. 44/11/3quinquies/2.

Abrogé

traitement des informations et des données à caractère personnel contenues dans les banques de données visées à l'article 44/2, § 2, est assuré conjointement par:

1° l'Organe de contrôle;

2° le Comité permanent de contrôle des services de renseignement et de sécurité, visé à l'article 28 de la loi organique, du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace.

Ils peuvent à tout moment émettre les recommandations qu'ils estiment nécessaires pour les traitements réalisés dans les banques de données communes.

Art. 44/11/9bis (nouveau)

Lorsque dans leurs missions de police administrative ou de police judiciaire, les membres des services de police sont appelés à coopérer avec les services de la santé, d'urgence et/ou de secours, ils peuvent communiquer des données à caractère personnel et des informations pour autant qu'elles soient adéquates, pertinentes et strictement nécessaires pour permettre aux membres des services de la de santé, d'urgence et/ou de secours, d'effectuer leurs missions dans des conditions de sécurité optimales et d'assurer la sécurité et l'intégrité psychologique et physique de toute personne dans l'exercice de ces fonctions.

Section 4 - Dispositions modificatives du Code consulaire

Art. 39/4

Le refus de délivrer une carte d'identité belge est levé:

1° dans les cas visés à l'article 39/2, § 1^{er}, 1°, dès que la mesure judiciaire limitative de liberté prend fin;

Art. 39/4

Le refus de délivrer une carte d'identité belge est levé:

1° dans les cas visés à l'article 39/2, § 1^{er}, 1°, dès que la mesure judiciaire limitative de liberté prend fin;

2° dans le cas visé à l'article 39/2, § 1er, 2°, après une décision de classement sans suite du ministère public, une ordonnance de non-lieu ou une décision finale de la juridiction d'instruction siégeant en tant que juridiction de jugement, ou un jugement ou arrêt passé en force de chose jugée à l'égard de l'intéressé;

3° dans le cas visé à l'article 39/2, § 1er, 3°, dès que la nationalité et l'identité du demandeur sont légalement établies;

4° dans le cas visé à l'article 39/2, § 2, dès que l'organe, le service ou l'organisme compétent à cet effet conclut que le demandeur ne présente manifestement plus un risque ou une menace substantiels pour l'ordre public ou la sécurité publique.

Le ministère public communique d'initiative au ministre l'identité des Belges qui tombent sous les catégories visées aux 1° et 2°. Les organes, services et organismes belges compétents communiquent d'initiative au ministre l'identité des Belges qui tombent sous la catégorie visée au 4°.

Dans le cas visé au 1°, le ministre peut toutefois, si le demandeur était impliqué dans des faits qui correspondent aux critères visés à l'article 6, § 1er, 1° ou 1° /1, de l'arrêté royal du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters, consulter l'organe, le service ou l'organisme compétent visé à l'article 39/2, § 2, afin de vérifier si le refus de délivrer une carte d'identité belge ne doit pas être maintenu sur la base de l'article 39/2, § 2

2° dans le cas visé à l'article 39/2, § 1er, 2°, après une décision de classement sans suite du ministère public, une ordonnance de non-lieu ou une décision finale de la juridiction d'instruction siégeant en tant que juridiction de jugement, ou un jugement ou arrêt passé en force de chose jugée à l'égard de l'intéressé;

3° dans le cas visé à l'article 39/2, § 1er, 3°, dès que la nationalité et l'identité du demandeur sont légalement établies;

4° dans le cas visé à l'article 39/2, § 2, dès que l'organe, le service ou l'organisme compétent à cet effet conclut que le demandeur ne présente manifestement plus un risque ou une menace substantiels pour l'ordre public ou la sécurité publique.

Le ministère public communique d'initiative au ministre l'identité des Belges qui tombent sous les catégories visées aux 1° et 2°. Les organes, services et organismes belges compétents communiquent d'initiative au ministre l'identité des Belges qui tombent sous la catégorie visée au 4°.

Dans le cas visé au 1°, le ministre peut toutefois, si le demandeur était impliqué dans des faits qui correspondent aux critères visés à l'article 2, 7° ou 8°, de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. ») et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police, consulter l'organe, le service ou l'organisme compétent visé à l'article 39/2, § 2, afin de vérifier si le refus de délivrer une carte d'identité belge ne doit pas être maintenu sur la base de l'article 39/2, § 2

Art. 65/1

Le refus de délivrer un passeport ou un titre de voyage belge est levé:

1° dans les cas visés à l'article 63, § 1^{er}, 1°, dès que la mesure judiciaire limitative de liberté prend fin;

2° dans le cas visé à l'article 63, § 1^{er}, 2°, après une décision de classement sans suite du ministère public, une ordonnance de non-lieu ou une décision finale, de la juridiction d'instruction siégeant en tant que juridiction de jugement, ou un jugement ou arrêt passé en force de chose jugée à l'égard de l'intéressé;

3° dans le cas visé à l'article 63, § 1^{er}, 3°, dès que la nationalité et l'identité du demandeur sont légalement établies;

4° dans le cas visé à l'article 63, § 1^{er}, 4°, dès que, conformément à l'article 374/1 du Code civil, soit les deux parents ou le parent qui exerce seul l'autorité parentale sur un enfant mineur non émancipé, respectivement donnent leur accord ou donne son accord pour la délivrance du passeport ou du titre de voyage à l'enfant, soit que le juge compétent donne son accord pour cette délivrance;

5° dans le cas visé à l'article 63, § 2, dès que l'organe, le service ou l'organisme compétent à cet effet conclut que le demandeur ne présente plus manifestement un risque ou une menace substantiels pour l'ordre public ou la sécurité publique.

Le ministère public communique d'initiative au ministre l'identité des Belges qui tombent sous les catégories visées aux 1° et 2°. Le greffier du tribunal de famille communique d'initiative au ministre l'identité des enfants mineurs belges qui tombent sous la catégorie visée au 4°, pour autant qu'il s'agit d'une décision du tribunal de famille. Les organes, services et organismes belges compétents communiquent d'initiative au ministre l'identité des Belges qui tombent sous la catégorie visée au 5°.

Art. 65/1

Le refus de délivrer un passeport ou un titre de voyage belge est levé:

1° dans les cas visés à l'article 63, § 1^{er}, 1°, dès que la mesure judiciaire limitative de liberté prend fin;

2° dans le cas visé à l'article 63, § 1^{er}, 2°, après une décision de classement sans suite du ministère public, une ordonnance de non-lieu ou une décision finale, de la juridiction d'instruction siégeant en tant que juridiction de jugement, ou un jugement ou arrêt passé en force de chose jugée à l'égard de l'intéressé;

3° dans le cas visé à l'article 63, § 1^{er}, 3°, dès que la nationalité et l'identité du demandeur sont légalement établies;

4° dans le cas visé à l'article 63, § 1^{er}, 4°, dès que, conformément à l'article 374/1 du Code civil, soit les deux parents ou le parent qui exerce seul l'autorité parentale sur un enfant mineur non émancipé, respectivement donnent leur accord ou donne son accord pour la délivrance du passeport ou du titre de voyage à l'enfant, soit que le juge compétent donne son accord pour cette délivrance;

5° dans le cas visé à l'article 63, § 2, dès que l'organe, le service ou l'organisme compétent à cet effet conclut que le demandeur ne présente plus manifestement un risque ou une menace substantiels pour l'ordre public ou la sécurité publique.

Le ministère public communique d'initiative au ministre l'identité des Belges qui tombent sous les catégories visées aux 1° et 2°. Le greffier du tribunal de famille communique d'initiative au ministre l'identité des enfants mineurs belges qui tombent sous la catégorie visée au 4°, pour autant qu'il s'agit d'une décision du tribunal de famille. Les organes, services et organismes belges compétents communiquent d'initiative au ministre l'identité des Belges qui tombent sous la catégorie visée au 5°.

Dans le cas visé au 1°, le ministre peut toutefois, si le demandeur était impliqué dans des faits qui correspondent aux critères visés à l'article 6, § 1^{er}, 1° ou 1° /1, de l'arrêté royal du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters, consulter l'organe, le service ou l'organisme compétent visé à l'article 63, § 2, afin de vérifier si le refus de délivrer un passeport ou un titre de voyage belge ne doit pas être maintenu sur la base de l'article 63, § 2

Dans le cas visé au 1°, le ministre peut toutefois, si le demandeur était impliqué dans des faits qui correspondent aux critères visés à l'article 2, 7° ou 8°, de la loi du [DATE] portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. ») et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police, consulter l'organe, le service ou l'organisme compétent visé à l'article 63, § 2, afin de vérifier si le refus de délivrer un passeport ou un titre de voyage belge ne doit pas être maintenu sur la base de l'article 63, § 2

Coördinatie van de artikelen

BASISTEKST

TEKST AANGEPAST AAN HET
WETSONTWERP

Hoofdstuk 4 – Wijzigingsbepalingen

Afdeling 1 – Wijzigingsbepalingen van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens

Art. 11.

§ 1. In toepassing van artikel 23 van de Verordening, zijn de artikelen 12 tot 22 en 34 van de Verordening alsook het principe van transparantie van de verwerking bedoeld in artikel 5 van de Verordening, niet van toepassing op verwerkingen van persoonsgegevens rechtstreeks of onrechtstreeks afkomstig van de overheden bedoeld in titel 3, ten aanzien van :

1° de overheden en personen bedoeld in artikelen 14, 16 en 19 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten naar wie deze gegevens rechtstreeks of onrechtstreeks werden overgebracht door de overheden bedoeld in titel 3;

2° de overheden en personen bedoeld in artikel 2, eerste lid, 2°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging en in artikel 44/11/3ter, §§ 2 en 3, en artikel 44/11/3quater van de wet van 5 augustus 1992 op het politieambt, en die onder het toepassingsgebied van titel 1 vallen, en aan wie deze gegevens werden overgemaakt.

Art. 11.

§ 1. In toepassing van artikel 23 van de Verordening, zijn de artikelen 12 tot 22 en 34 van de Verordening alsook het principe van transparantie van de verwerking bedoeld in artikel 5 van de Verordening, niet van toepassing op verwerkingen van persoonsgegevens rechtstreeks of onrechtstreeks afkomstig van de overheden bedoeld in titel 3, ten aanzien van :

1° de overheden en personen bedoeld in artikelen 14, 16 en 19 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten naar wie deze gegevens rechtstreeks of onrechtstreeks werden overgebracht door de overheden bedoeld in titel 3;

2° de overheden en personen bedoeld in artikel 2, eerste lid, 2°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging en in de artikelen 16 en 23, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”) en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt, en die onder het toepassingsgebied van titel 1 vallen, en aan wie deze gegevens werden overgemaakt.

§ 2. De verwerkingsverantwoordelijke bedoeld in deze titel die in het bezit is van zulke gegevens deelt deze niet mee aan de betrokkene tenzij :

1° de wet hem hiertoe verplicht in het kader van een geschillenprocedure; of

2° de betrokken overheid bedoeld in titel 3 hem dit toestaat.

De verwerkingsverantwoordelijke of de bevoegde overheid deelt niet mee dat hij in het bezit is van gegevens die van overheden bedoeld in titel 3 afkomstig zijn.

§ 3. De beperkingen bedoeld in paragraaf 1 hebben eveneens betrekking op de logbestanden van de verwerkingen van een overheid bedoeld in titel 3 in de gegevensbanken van de verwerkingsverantwoordelijken bedoeld in deze titel waartoe de overheid rechtstreeks toegang heeft.

§ 4. De verwerkingsverantwoordelijke bedoeld in deze titel die gegevens verwerkt die rechtstreeks of onrechtstreeks afkomstig zijn van de overheden bedoeld in titel 3 beantwoordt minstens aan de volgende voorwaarden :

1° hij neemt de gepaste technische of organisatorische maatregelen om ervoor te zorgen dat de toegang tot de gegevens en de verwerkingsmogelijkheden beperkt zijn tot hetgeen de personen nodig hebben om hun functies uit te oefenen of tot hetgeen nodig is voor de behoeften van de dienst;

2° hij neemt de gepaste technische of organisatorische maatregelen om de persoonsgegevens te beschermen tegen toevallige of niet-toegestane vernietiging, tegen toevallig verlies en tegen wijziging of elke andere niet-toegestane verwerking van die gegevens.

De leden van het personeel van de verwerkingsverantwoordelijke die de gegevens bedoeld in het eerste lid verwerken, zijn bovendien gebonden door de discretieplicht.

§ 2. De verwerkingsverantwoordelijke bedoeld in deze titel die in het bezit is van zulke gegevens deelt deze niet mee aan de betrokkene tenzij :

1° de wet hem hiertoe verplicht in het kader van een geschillenprocedure; of

2° de betrokken overheid bedoeld in titel 3 hem dit toestaat.

De verwerkingsverantwoordelijke of de bevoegde overheid deelt niet mee dat hij in het bezit is van gegevens die van overheden bedoeld in titel 3 afkomstig zijn.

§ 3. De beperkingen bedoeld in paragraaf 1 hebben eveneens betrekking op de logbestanden van de verwerkingen van een overheid bedoeld in titel 3 in de gegevensbanken van de verwerkingsverantwoordelijken bedoeld in deze titel waartoe de overheid rechtstreeks toegang heeft.

§ 4. De verwerkingsverantwoordelijke bedoeld in deze titel die gegevens verwerkt die rechtstreeks of onrechtstreeks afkomstig zijn van de overheden bedoeld in titel 3 beantwoordt minstens aan de volgende voorwaarden :

1° hij neemt de gepaste technische of organisatorische maatregelen om ervoor te zorgen dat de toegang tot de gegevens en de verwerkingsmogelijkheden beperkt zijn tot hetgeen de personen nodig hebben om hun functies uit te oefenen of tot hetgeen nodig is voor de behoeften van de dienst;

2° hij neemt de gepaste technische of organisatorische maatregelen om de persoonsgegevens te beschermen tegen toevallige of niet-toegestane vernietiging, tegen toevallig verlies en tegen wijziging of elke andere niet-toegestane verwerking van die gegevens.

De leden van het personeel van de verwerkingsverantwoordelijke die de gegevens bedoeld in het eerste lid verwerken, zijn bovendien gebonden door de discretieplicht.

§ 5. Wanneer een verzoek of een klacht aanhangig wordt gemaakt bij de toezichthoudende autoriteit bedoeld in de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, waarbij de verwerkingsverantwoordelijke melding maakt van de toepassing van dit artikel, wendt de toezichthoudende autoriteit eerste zich tot het Vast Comité I opdat het de nodige verificaties verricht bij de autoriteit bedoeld in titel 3.

Na ontvangst van het antwoord van het Vast Comité I, brengt de Gegevensbeschermingsautoriteit de betrokkene enkel op de hoogte van de resultaten van de verificatie die betrekking hebben op persoonsgegevens die niet van de autoriteiten bedoeld in titel 3 afkomstig zijn, die de toezichthoudende autoriteit wettelijk gehouden is mee te delen.

Indien het verzoek of de klacht enkel betrekking heeft op persoonsgegevens afkomstig van een autoriteit bedoeld in titel 3, antwoordt de Gegevensbeschermingsautoriteit, na ontvangst van het antwoord van het Vast Comité I, dat de nodige verificaties werden verricht.

ONDERTITEL 4. - De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door het coördinatieorgaan voor de dreigingsanalyse

Art. 138.

§ 1. De definities bedoeld in de artikelen 26, 1° tot 6°, 9°, 11° tot 14° en 16° tot 17°, zijn van toepassing op deze ondertitel.

§ 2. Voor de toepassing van deze ondertitel wordt verstaan onder :

1° "het OCAD" : het Coördinatieorgaan voor de dreigingsanalyse bedoeld in de wet van

§ 5. Wanneer een verzoek of een klacht aanhangig wordt gemaakt bij de toezichthoudende autoriteit bedoeld in de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, waarbij de verwerkingsverantwoordelijke melding maakt van de toepassing van dit artikel, wendt de toezichthoudende autoriteit eerste zich tot het Vast Comité I opdat het de nodige verificaties verricht bij de autoriteit bedoeld in titel 3.

Na ontvangst van het antwoord van het Vast Comité I, brengt de Gegevensbeschermingsautoriteit de betrokkene enkel op de hoogte van de resultaten van de verificatie die betrekking hebben op persoonsgegevens die niet van de autoriteiten bedoeld in titel 3 afkomstig zijn, die de toezichthoudende autoriteit wettelijk gehouden is mee te delen.

Indien het verzoek of de klacht enkel betrekking heeft op persoonsgegevens afkomstig van een autoriteit bedoeld in titel 3, antwoordt de Gegevensbeschermingsautoriteit, na ontvangst van het antwoord van het Vast Comité I, dat de nodige verificaties werden verricht.

ONDERTITEL 4. - De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door het coördinatieorgaan voor de dreigingsanalyse en de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces"

Art. 138.

§ 1. De definities bedoeld in de artikelen 26, 1° tot 6°, 9°, 11° tot 14° en 16° tot 17°, zijn van toepassing op deze ondertitel.

§ 2. Voor de toepassing van deze ondertitel wordt verstaan onder :

1° "het OCAD" : het Coördinatieorgaan voor de dreigingsanalyse bedoeld in de wet van

10 juli 2006 betreffende de analyse van de dreiging;

2° "de verwerkingsverantwoordelijke" : een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;

3° "de wet van 18 juli 1991" : de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;

4° "de wet van 11 december 1998" : de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

5° "toezichthoudende autoriteit" : een onafhankelijke overheidsinstantie die bij de wet belast is met het toezicht op de toepassing van deze wet;

6° "de wet van 10 juli 2006" : de wet van 10 juli 2006 betreffende de analyse van de dreiging;

7° "het informatiesysteem van het OCAD" : het informatiesysteem bedoeld in artikel 9 van de wet van 10 juli 2006.

10 juli 2006 betreffende de analyse van de dreiging;

2° "de verwerkingsverantwoordelijke" : een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;

3° "de wet van 18 juli 1991" : de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;

4° "de wet van 11 december 1998" : de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

5° "toezichthoudende autoriteit" : een onafhankelijke overheidsinstantie die bij de wet belast is met het toezicht op de toepassing van deze wet;

6° "de wet van 10 juli 2006" : de wet van 10 juli 2006 betreffende de analyse van de dreiging;

7° "het informatiesysteem van het OCAD" : het informatiesysteem bedoeld in artikel 9 van de wet van 10 juli 2006;

8° "de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.")": de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R."). en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt;

9° "de gemeenschappelijke gegevensbank "T.E.R."": de

gegevensbank bedoeld in artikel 3 van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”) ;

10° “de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank “T.E.R.””: de verwerkingsverantwoordelijken bedoeld in artikel 5, eerste lid, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”).

Art. 139

Deze ondertitel is van toepassing op elke verwerking van persoonsgegevens door het OCAD en zijn verwerkers, uitgevoerd in het kader van de opdrachten als bedoeld in de wet van 10 juli 2006, en door of krachtens bijzondere wetten.

De titels 1, 2, 4, 5 en 7 van deze wet zijn niet van toepassing op de verwerkingen bedoeld in het eerste lid. In titel 6 zijn enkel de artikelen 226, 227 en 230 van toepassing.

Art. 139

Deze ondertitel is van toepassing op elke verwerking van persoonsgegevens door het OCAD en zijn verwerkers, uitgevoerd in het kader van de opdrachten als bedoeld in de wet van 10 juli 2006, en door of krachtens bijzondere wetten **en op elke verwerking van persoonsgegevens in de gemeenschappelijke gegevensbank “T.E.R.”.**

De titels 1, 2, 4, 5 en 7 van deze wet zijn niet van toepassing op de verwerkingen bedoeld in het eerste lid. In titel 6 zijn enkel de artikelen 226, 227 en 230 van toepassing.

Art. 140

Persoonsgegevens mogen slechts verwerkt worden in één van de volgende gevallen :

1° wanneer de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend;

2° wanneer de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor de uitvoering van maatregelen die aan het sluiten van die overeenkomst voorafgaan en die op verzoek van de betrokkene zijn genomen;

Art. 140

Persoonsgegevens mogen slechts verwerkt worden in één van de volgende gevallen :

1° wanneer de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend;

2° wanneer de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor de uitvoering van maatregelen die aan het sluiten van die overeenkomst voorafgaan en die op verzoek van de betrokkene zijn genomen;

3° wanneer de verwerking nuttig is om een verplichting na te komen waaraan het OCAD is onderworpen door of krachtens een wet;

4° wanneer de verwerking noodzakelijk is voor de vervulling van een taak van openbaar belang of die deel uitmaakt van de uitoefening van het openbaar gezag, die is opgedragen aan de verwerkingsverantwoordelijke of aan de overheidsinstantie aan wie de persoonsgegevens worden verstrekt.

3° wanneer de verwerking nuttig is om een verplichting na te komen waaraan het OCAD is onderworpen door of krachtens een wet;

4° wanneer de verwerking noodzakelijk is voor de vervulling van een taak van openbaar belang of die deel uitmaakt van de uitoefening van het openbaar gezag, die is opgedragen aan de verwerkingsverantwoordelijke of aan de overheidsinstantie aan wie de persoonsgegevens worden verstrekt.

5° wanneer de verwerking nuttig is in het kader van de doeleinden bedoeld in artikel 5, tweede lid, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.").

Art. 143.

De persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor ze opgeslagen worden en volgens de nadere regels bepaald in artikel 9 van de wet van 10 juli 2006 voor wat het informatiesysteem van het OCAD betreft en artikel 44/11/3bis van de wet van 5 augustus 1992 op het politieambt voor wat betreft de gemeenschappelijke gegevensbanken waarvan het OCAD de operationele beheerder is.

Art. 143.

De persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor ze opgeslagen worden en volgens de nadere regels bepaald in artikel 9 van de wet van 10 juli 2006 voor wat het informatiesysteem van het OCAD betreft en artikel 7 van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.") voor wat betreft de gemeenschappelijke gegevensbank "T.E.R.".

Art. 147

De toezichthoudende autoriteiten bedoeld in artikel 161 en het OCAD houden een logbestand bij van alle aanvragen van betrokkenen tot uitoefening van hun rechten.

Art. 147

De toezichthoudende autoriteiten bedoeld in artikel 161 de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R." en het OCAD houden een logbestand bij van alle aanvragen van betrokkenen tot uitoefening van hun rechten.

Art. 149

Art. 149

De verwerkingsverantwoordelijke :

1° waakt er nauwlettend over dat de persoonsgegevens worden bijgewerkt, dat de onjuiste, onvolledige en niet terzake dienende gegevens, alsmede die welke zijn verkregen of verder verwerkt in strijd met deze ondertitel, worden verbeterd of verwijderd;

2° zorgt ervoor dat voor de personen die onder zijn gezag handelen, de toegang tot de persoonsgegevens en de verwerkingsmogelijkheden, beperkt blijven tot wat nuttig is voor de uitoefening van hun opdrachten of voor de behoeften van het OCAD;

3° informeert alle personen die onder zijn gezag handelen over de bepalingen van deze ondertitel en over alle relevante voorschriften inzake de bescherming van de persoonlijke levenssfeer betreffende de verwerking van persoonsgegevens.

Art. 155

§ 1. Indien een inbreuk op de beveiliging een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt, meldt de verwerkingsverantwoordelijke deze inbreuk binnen de kortste termijn aan de bevoegde toezichthoudende autoriteit en indien mogelijk, 72 uur nadat hij er kennis van heeft genomen.

§ 2. De verwerker verwittigt de verwerkingsverantwoordelijke binnen de kortste termijn van elke inbreuk op de beveiliging.

De verwerkingsverantwoordelijke :

1° waakt er nauwlettend over dat de persoonsgegevens worden bijgewerkt, dat de onjuiste, onvolledige en niet terzake dienende gegevens, alsmede die welke zijn verkregen of verder verwerkt in strijd met deze ondertitel, worden verbeterd of verwijderd;

2° zorgt ervoor dat voor de personen die onder zijn gezag handelen, de toegang tot de persoonsgegevens en de verwerkingsmogelijkheden, beperkt blijven tot wat nuttig is voor de uitoefening van hun opdrachten of voor de behoeften van het OCAD of in het kader van de doeleinden van de gemeenschappelijke gegevensbank "T.E.R." bedoeld in artikel 5, tweede lid, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.");

3° informeert alle personen die onder zijn gezag handelen over de bepalingen van deze ondertitel en over alle relevante voorschriften inzake de bescherming van de persoonlijke levenssfeer betreffende de verwerking van persoonsgegevens.

Art. 155

§ 1. Onder voorbehoud van de bepalingen van artikel 13 van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.") meldt de betrokken verwerkingsverantwoordelijke een inbreuk op de beveiliging die een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt, binnen de kortste termijn en indien mogelijk 72 uur nadat hij er kennis van heeft genomen, aan de bevoegde toezichthoudende overheid.

§ 2. De verwerker verwittigt de verwerkingsverantwoordelijke binnen de kortste termijn van elke inbreuk op de beveiliging.

§ 3. In de in paragrafen 1 en 2 bedoelde melding wordt, op zijn minst, het volgende omschreven of meegedeeld :

1° de aard van de inbreuk op de beveiliging en indien mogelijk, bij benadering, het aantal betrokkenen en de opgeslagen persoonsgegevens in kwestie;

2° de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt bij wie bijkomende informatie kan worden verkregen;

3° de waarschijnlijke gevolgen van de inbreuk op de beveiliging;

4° de maatregelen die de verwerkingsverantwoordelijke, of de verwerker heeft genomen of voorgesteld om de inbreuk op de beveiliging aan te pakken, waaronder desgevallend maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

§ 3. In de in paragrafen 1 en 2 bedoelde melding wordt, op zijn minst, het volgende omschreven of meegedeeld :

1° de aard van de inbreuk op de beveiliging en indien mogelijk, bij benadering, het aantal betrokkenen en de opgeslagen persoonsgegevens in kwestie;

2° de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt bij wie bijkomende informatie kan worden verkregen;

3° de waarschijnlijke gevolgen van de inbreuk op de beveiliging;

4° de maatregelen die de verwerkingsverantwoordelijke, of de verwerker heeft genomen of voorgesteld om de inbreuk op de beveiliging aan te pakken, waaronder desgevallend maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Art. 156

§ 1. De verwerkingsverantwoordelijke houdt een register bij, geclassificeerd in de zin van de wet van 11 december 1998, van de gegevensbanken van het OCAD en deze die aan hem ter beschikking worden gesteld.

Dit register bevat de volgende gegevens :

1° voor de gegevensbanken van het OC Opheffing :

a) de contactgegevens van de verwerkingsverantwoordelijke en, desgevallend, van de gezamenlijke verwerkingsverantwoordelijken, en van de functionaris voor gegevensbescherming;

b) de verwerkingsdoeleinden;

c) de categorieën van ontvangers waaraan persoonsgegevens meegedeeld kunnen worden;

Art. 156

§ 1. De verwerkingsverantwoordelijke houdt een register bij, geclassificeerd in de zin van de wet van 11 december 1998, **van de gemeenschappelijke gegevensbank "T.E.R."**, van de gegevensbanken van het OCAD en deze die aan hem ter beschikking worden gesteld.

Dit register bevat de volgende gegevens :

1° voor de gemeenschappelijke gegevensbank "T.E.R." en de gegevensbanken van het OCAD :

a) de contactgegevens van de verwerkingsverantwoordelijke en, desgevallend, van de gezamenlijke verwerkingsverantwoordelijken, en van de functionaris voor gegevensbescherming;

b) de verwerkingsdoeleinden;

c) de categorieën van ontvangers waaraan persoonsgegevens meegedeeld kunnen worden;

d) indien mogelijk, de beoogde termijnen voor het verwijderen van de persoonsgegevens;

e) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 154;

2° Voor gegevensbanken die aan het OCAD ter beschikking gesteld worden :

a) de contactgegevens van de verwerkingsverantwoordelijke en, indien mogelijk voor de landen buiten de Europese Unie de dienst die de gegevensbank beheert en, desgevallend, van de gezamenlijke verwerkingsverantwoordelijken en van de functionaris voor gegevensbescherming;

b) de verwerkingsdoeleinden van het OCAD.

§ 2. Elke verwerker houdt een register bij, geclassificeerd in de zin van de wet van 11 december 1998, van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht.

Dit register bevat de volgende elementen :

1° de contactgegevens van de verwerker en van de verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt, en, desgevallend, van de functionaris voor gegevensbescherming;

2° de categorieën van verwerkingen die voor rekening van de verwerkingsverantwoordelijke zijn uitgevoerd;

3° indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 154.

§ 3. De in de paragrafen 1 en 2 bedoelde registers worden in schriftelijke vorm, met inbegrip van elektronische vorm, opgesteld.

d) indien mogelijk, de beoogde termijnen voor het verwijderen van de persoonsgegevens;

e) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 154;

2° Voor gegevensbanken die aan het OCAD ter beschikking gesteld worden :

a) de contactgegevens van de verwerkingsverantwoordelijke en, indien mogelijk voor de landen buiten de Europese Unie de dienst die de gegevensbank beheert en, desgevallend, van de gezamenlijke verwerkingsverantwoordelijken en van de functionaris voor gegevensbescherming;

b) de verwerkingsdoeleinden van het OCAD.

§ 2. Elke verwerker houdt een register bij, geclassificeerd in de zin van de wet van 11 december 1998, van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht.

Dit register bevat de volgende elementen :

1° de contactgegevens van de verwerker en van de verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt, en, desgevallend, van de functionaris voor gegevensbescherming;

2° de categorieën van verwerkingen die voor rekening van de verwerkingsverantwoordelijke zijn uitgevoerd;

3° indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen bedoeld in artikel 154.

§ 3. De in de paragrafen 1 en 2 bedoelde registers worden in schriftelijke vorm, met inbegrip van elektronische vorm, opgesteld.

§ 4. De verwerkingsverantwoordelijke stelt het register ter beschikking van de bevoegde toezichthoudende autoriteit op diens vraag.

De verwerker stelt het register ter beschikking van de verwerkingsverantwoordelijke en stelt het eveneens ter beschikking van de bevoegde toezichthoudende autoriteit op diens vraag.

§ 4. De verwerkingsverantwoordelijke stelt het register ter beschikking van de bevoegde toezichthoudende autoriteit op diens vraag.

De verwerker stelt het register ter beschikking van de verwerkingsverantwoordelijke en stelt het eveneens ter beschikking van de bevoegde toezichthoudende autoriteit op diens vraag.

Art. 157/1 (nieuw)

§1. De gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R.", en desgevallend de verwerker, wijzen een functionaris voor gegevensbescherming aan. Deze beslissing wordt meegedeeld aan de bevoegde toezichthoudende autoriteiten.

De functionaris voor gegevensbescherming is titularis van een veiligheidsmachtiging "geheim", in de zin van de wet van 11 december 1998.

§ 2. De functionaris voor gegevensbescherming kan niet gestraft worden voor het uitoefenen van zijn functie. Hij kan evenmin van zijn functie ontheven worden omwille van de uitvoering van zijn opdrachten, behalve indien hij een zware fout heeft begaan of de voorwaarden noodzakelijk voor het uitoefenen van zijn functie niet langer vervult.

De functionaris voor gegevensbescherming kan zich tot het Controleorgaan op de Politie Informatie of het Vast Comité I wenden om deze beslissing aan te vechten.

§ 3. Hij is, op een onafhankelijke wijze, belast met :

1° het toezien op de naleving van deze ondertitel bij elke verwerking van persoonsgegevens in het kader van de gemeenschappelijke gegevensbank "T.E.R.";

2° het adviseren over alle nuttige maatregelen teneinde de veiligheid van de opgeslagen gegevens in de gemeenschappelijke gegevensbank "T.E.R." te verzekeren;

3° het informeren en adviseren van de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R.", en desgevallend de beheerder, de operationeel verantwoordelijke, de verwerker, het diensthoofd en de personeelsleden van de betrokken dienst die de verwerking verrichten over hun verplichtingen op grond van deze ondertitel en de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.");

4° het verstrekken van adviezen of aanbevelingen aan de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R.", en desgevallend aan de beheerder, de operationeel verantwoordelijke en de verwerker;

5° het uitvoeren van andere opdrachten die hem door de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R.", en in voorkomend geval de operationeel verantwoordelijke.

§4. De functionaris voor gegevensbescherming:

1° waakt over de bewustmaking van de gebruikers inzake bescherming van de persoonsgegevens en de veiligheid;

2° werkt samen met de beheerder in het kader van het uitwerken van procedures;

3° werkt, indien nodig, samen met de functionarissen voor de gegevensbescherming van de diensten die de gegevens in de gemeenschappelijke gegevensbank "T.E.R." verwerken;

4° is de contactpersoon met de toezichthoudende autoriteiten voor aangelegenheden in verband met de verwerkingen die in de gemeenschappelijke gegevensbank "T.E.R." worden uitgevoerd.

§5. De functionaris voor gegevensbescherming oefent zijn functies uit in alle onafhankelijkheid en met inachtneming van de respectieve bevoegdheden en opdrachten van de basisdiensten en de partnerdiensten.

De gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R.", de beheerder en de operationeel verantwoordelijke zien erop toe dat de functionaris voor gegevensbescherming tijdig en op passende wijze betrokken wordt bij alle aangelegenheden in verband met de bescherming van persoonsgegevens.

De gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R." ziet erop toe dat de functionaris voor gegevensbescherming beschikt over de nodige middelen voor het vervullen van zijn opdrachten

De functionaris voor gegevensbescherming kan worden bijgestaan door een of meer adjuncten

Hij brengt rechtstreeks verslag uit aan de gezamenlijke verwerkingsverantwoordelijken van de gemeenschappelijke gegevensbank "T.E.R.", die de operationeel verantwoordelijke op de hoogte brengen.

§ 6. Desgevallend kunnen nadere regels voor de werking, de aanwijzing en de vereiste bevoegdheden van de functionaris voor gegevensbescherming door de Koning worden bepaald.

Art. 158

Art. 158

In afwijking van de artikelen 20, 22, 23, 58 en 59 van deze wet en van de artikelen 35 en 36 van de Verordening kan noch een protocol, noch een advies van de functionaris voor gegevensbescherming, noch een gegevensbeschermingseffectbeoordeling, noch het advies volgend op de raadpleging van de bevoegde toezichthoudende autoriteit vereist worden als voorafgaande voorwaarde voor de mededeling van persoonsgegevens tussen het OCAD en enig openbaar of particulier orgaan, in het belang van de uitvoering van de opdrachten van het OCAD.

Deze mededeling vindt plaats in overeenstemming met de artikelen 8 tot 12 van de wet van 10 juli 2006 en hoofdstuk IV, afdeling 12, onderafdeling 7bis, van de wet van 5 augustus 1992 op het politieambt.

Wanneer de partijen beslissen een protocol af te sluiten, bevat dit, in afwijking van artikel 20, § 1, tweede lid, het volgende :

1° de identificatie van het OCAD en het openbaar of particulier orgaan die de persoonsgegevens uitwisselen;

2° de identificatie van de verwerkingsverantwoordelijken;

3° de contactgegevens van de betrokken functionarissen voor gegevensbescherming;

4° de doeleinden waarvoor de persoonsgegevens worden doorgegeven;

5° de wettelijke grondslag;

6° de beperkingen van de rechten van de betrokkene.

Het protocol bedoeld in het derde lid draagt de markering "BEPERKTE VERSPREIDING" in de zin van het koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998, voor zover een classificatie in de zin van de wet van 11 december 1998 niet gerechtvaardigd is.

In afwijking van de artikelen 20, 22, 23, 58 en 59 van deze wet en van de artikelen 35 en 36 van de Verordening kan noch een protocol, noch een advies van de functionaris voor gegevensbescherming, noch een gegevensbeschermingseffectbeoordeling, noch het advies volgend op de raadpleging van de bevoegde toezichthoudende autoriteit vereist worden als voorafgaande voorwaarde voor de mededeling van persoonsgegevens tussen het OCAD en enig openbaar of particulier orgaan, in het belang van de uitvoering van de opdrachten van het OCAD.

In afwijking van de artikelen 20, 22, 23, 58 en 59 van deze wet en van de artikelen 35 en 36 van de Verordening kan noch een protocol, noch een advies van de functionaris voor gegevensbescherming, noch een gegevensbeschermingseffectbeoordeling, noch het advies volgend op de raadpleging van de bevoegde toezichthoudende autoriteit vereist worden als voorafgaande voorwaarde voor de mededeling van persoonsgegevens van de gemeenschappelijke gegevensbank "T.E.R." aan enig openbaar of particulier orgaan, in het belang van de uitvoering van de opdrachten inzake de voorkoming en de opvolging van terrorisme en extremisme, dat kan leiden tot terrorisme, bedoeld in artikel 3, eerste lid, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.").

De mededeling bedoeld in het eerste lid vindt plaats in overeenstemming met de artikelen 8 tot 12 van de wet van 10 juli 2006.

De mededeling bedoeld in het tweede lid vindt plaats in overeenstemming met de artikelen 20 tot 28 van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.").

Wanneer de partijen beslissen een protocol af te sluiten, bevat dit, in afwijking van artikel 20, paragraaf 1, tweede lid, het volgende :

1° de identificatie van het openbaar of particulier orgaan die de persoonsgegevens uitwisselen, en in voorkomend geval, de identificatie van het OCAD

2° de identificatie van de verwerkingsverantwoordelijken;

3° de contactgegevens van de betrokken functionarissen voor gegevensbescherming;

4° de doeleinden waarvoor de persoonsgegevens worden doorgegeven;

5° de wettelijke grondslag;

6° de beperkingen van de rechten van de betrokkene.

Het protocol bedoeld in het vijfde lid draagt de markering "BEPERKTE VERSPREIDING" in de zin van het koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998, voor zover een classificatie in de zin van de wet van 11 december 1998 niet gerechtvaardigd is."

Art. 161

Het Vast Comité I, in zijn hoedanigheid van onafhankelijke publieke autoriteit, en het Vast Comité van Toezicht op de politiediensten, worden aangewezen als gegevensbeschermingsautoriteiten belast met de controle van de verwerking van persoonsgegevens door het OCAD en zijn verwerkers volgens de nadere regels vastgelegd in de wet van 18 juli 1991.

Art. 161.

Het Vast Comité I, in zijn hoedanigheid van onafhankelijke publieke autoriteit, en het Vast Comité van Toezicht op de politiediensten, worden aangewezen als gegevensbeschermingsautoriteiten belast met de controle van de verwerking van persoonsgegevens door het OCAD en zijn verwerkers volgens de nadere regels vastgelegd in de wet van 18 juli 1991.

De toezichthoudende overheden bedoeld in artikel 2, 22°, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank

“Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”) worden gezamenlijk aangewezen als gegevensbeschermingsautoriteiten belast met de controle van de verwerking van persoonsgegevens in de gemeenschappelijke gegevensbank “T.E.R.”.

Art. 162

In afwijking van titel 4, wordt de raadpleging voor historische, wetenschappelijke of statistische doeleinden, door een verdere verwerkingsverantwoordelijke, van persoonsgegevens van het OCAD en van hun personeel toegestaan door het OCAD indien dit geen afbreuk doet aan zijn opdrachten bedoeld in de wet van 10 juli 2006, aan een lopend opsporings- of gerechtelijk onderzoek, of aan de betrekkingen die België met vreemde staten of internationale organisaties onderhoudt en overeenkomstig de wet van 10 juli 2006.

Elke vraag aan de Rijksarchieven om verdere verwerking van persoonsgegevens van het OCAD en van hun personeel voor overige doelen dan die bedoeld in het eerste lid wordt geweigerd tenzij het doel legitiem is en het OCAD meent dat de verwerking geen afbreuk kan doen aan de belangen bedoeld in het eerste lid.

Art. 162

In afwijking van titel 4, wordt de raadpleging voor historische, wetenschappelijke of statistische doeleinden, door een verdere verwerkingsverantwoordelijke, van persoonsgegevens van het OCAD en van hun personeel toegestaan door het OCAD indien dit geen afbreuk doet aan zijn opdrachten bedoeld in de wet van 10 juli 2006, aan een lopend opsporings- of gerechtelijk onderzoek, of aan de betrekkingen die België met vreemde staten of internationale organisaties onderhoudt en overeenkomstig de wet van 10 juli 2006.

Elke vraag aan de Rijksarchieven om verdere verwerking van persoonsgegevens van het OCAD en van hun personeel voor overige doelen dan die bedoeld in het eerste lid wordt geweigerd tenzij het doel legitiem is en het OCAD meent dat de verwerking geen afbreuk kan doen aan de belangen bedoeld in het eerste lid.

In afwijking van het eerste lid, wordt de raadpleging voor historische, wetenschappelijke of statistische doeleinden, door een verdere verwerkingsverantwoordelijke, van persoonsgegevens met betrekking tot de in de gemeenschappelijke gegevensbank “T.E.R.” geregistreerde entiteiten toestaan door de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank “T.E.R.” na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”). Wanneer de raadpleging de veiligheid van een persoon, de uitoefening van de

strafvordering, de uitoefening van een inlichtingenonderzoek of de relatie met een rechtshandavingsinstantie van een buitenlandse Staat of met een inlichtingen- en veiligheidsdienst van een buitenlandse Staat in het gedrang kan brengen, wordt ze automatisch geweigerd.

Elke vraag aan de Rijksarchieven om verdere verwerking van persoonsgegevens geregistreerd in de gemeenschappelijke gegevensbank "T.E.R." voor overige doelen dan die bedoeld in het derde lid wordt geweigerd tenzij het doel, legitiem is, er geen onevenredige afbreuk wordt gedaan aan het privéleven en na advies van de operationeel verantwoordelijke.

Art. 164

De persoonsgegevens bedoeld in artikel 162 worden voorafgaand aan hun raadpleging geanonimiseerd.

Indien een verdere verwerking van anonieme gegevens niet toelaat om de historische, wetenschappelijke of statistische doeleinden te verwezenlijken, kan het OCAD de raadpleging van gepseudonimiseerde gegevens toestaan.

Indien de anonimisering of pseudonimisering de identificatie van de gegevens niet onmogelijk maakt, weigert het OCAD de raadpleging indien dit een onevenredige afbreuk doet aan het privéleven.

Indien een verdere verwerking van gepseudonimiseerde gegevens niet toelaat om de historische, wetenschappelijke of statistische doeleinden te verwezenlijken, kan het OCAD de raadpleging van niet-gepseudonimiseerde gegevens toestaan indien dit geen onevenredige afbreuk doet aan het privéleven.

Art. 164

De persoonsgegevens bedoeld in artikel 162 worden voorafgaand aan hun raadpleging geanonimiseerd.

Indien een verdere verwerking van anonieme gegevens niet toelaat om de historische, wetenschappelijke of statistische doeleinden te verwezenlijken, kan het OCAD of de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank "T.E.R." na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R."), wat betreft de gemeenschappelijke gegevensbank "T.E.R.", de raadpleging van gepseudonimiseerde gegevens toestaan.

Indien de anonimisering of pseudonimisering de identificatie van de gegevens niet onmogelijk maakt, weigert het OCAD of de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank "T.E.R." na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van [DATUM] tot oprichting van de

gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”), wat betreft de gemeenschappelijke gegevensbank “T.E.R.”, de raadpleging indien dit een onevenredige afbreuk doet aan het privéleven.

Indien een verdere verwerking van gepseudonimiseerde gegevens niet toelaat om de historische, wetenschappelijke of statistische doeleinden te verwezenlijken, kan het OCAD of de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank “T.E.R.” na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”), wat betreft de gemeenschappelijke gegevensbank “T.E.R.”, de raadpleging van niet-gepseudonimiseerde gegevens toestaan indien dit geen onevenredige afbreuk doet aan het privéleven.

Art. 165

In afwijking van titel 4, is een mededeling of publicatie van niet-geanonimiseerde of niet-gepseudonimiseerde persoonsgegevens bedoeld in artikel 162, geraadpleegd door de verdere verwerkingsverantwoordelijke, is enkel mogelijk met het akkoord van het OCAD en onder de voorwaarden die het vastlegt.

Art. 165

In afwijking van titel 4, is een mededeling of publicatie van niet-geanonimiseerde of niet-gepseudonimiseerde persoonsgegevens bedoeld in artikel 162, geraadpleegd door de verdere verwerkingsverantwoordelijke, is enkel mogelijk met het akkoord van het OCAD of de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank “T.E.R.” na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”), wat betreft de gemeenschappelijke gegevensbank “T.E.R.”, en onder de voorwaarden die het vastlegt.

Art. 166

Art. 166

De verdere verwerkingsverantwoordelijke van persoonsgegevens bedoeld in artikel 162 houdt een logbestand van zijn verdere verwerkingsactiviteiten voor historische, wetenschappelijke of statistische doeleinden bij.

Dit logbestand is geclassificeerd in de zin van de wet van 11 december 1998 indien de verwerking betrekking heeft op geclassificeerde gegevens.

Dit logbestand bevat de volgende informatie :

1° de contactgegevens van de eerste verwerkingsverantwoordelijke, de verdere verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming van deze laatste;

2° de doeleinden van de verdere verwerking;

3° de gegevens die het voorwerp uitmaken van de verdere verwerking;

4° de eventuele voorwaarden voor de verdere verwerking vastgelegd door het OCAD;

5° de eventuele ontvangers toegestaan door het OCAD.

De verdere verwerkingsverantwoordelijke van persoonsgegevens bedoeld in artikel 162 houdt een logbestand van zijn verdere verwerkingsactiviteiten voor historische, wetenschappelijke of statistische doeleinden bij.

Dit logbestand is geclassificeerd in de zin van de wet van 11 december 1998 indien de verwerking betrekking heeft op geclassificeerde gegevens.

Dit logbestand bevat de volgende informatie :

1° de contactgegevens van de eerste verwerkingsverantwoordelijke, de verdere verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming van deze laatste;

2° de doeleinden van de verdere verwerking;

3° de gegevens die het voorwerp uitmaken van de verdere verwerking;

4° de eventuele voorwaarden voor de verdere verwerking vastgelegd door het OCAD **of door de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank "T.E.R." na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R."), wat betreft de gemeenschappelijke gegevensbank "T.E.R.";**

5° de eventuele ontvangers toegestaan door het OCAD **of door de operationeel verantwoordelijke van de gemeenschappelijke gegevensbank "T.E.R." na overleg met de basisdiensten bedoeld in artikel 2, 2° van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R."), wat betreft de gemeenschappelijke gegevensbank "T.E.R.".**

Afdeling 2 – Wijzigingsbepaling van de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme

Art. 4.

§ 1. De korpschef en/of de door hem aangestelde vertegenwoordiger van de lokale politie bedoeld in artikel 3, kan de informatiekaarten, zoals bedoeld in artikel 1, 15°, van het koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1bis "het informatiebeheer" van hoofdstuk IV van de wet op het politieambt en artikel 1, 12°, van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Terrorist Fighters, van de personen van wie het geval ter bespreking wordt voorgelegd in een LIVC R overeenkomstig artikel 3, § 2, meedelen aan de leden van het LIVC R.

§ 2. De korpschef en/of de door hem aangestelde vertegenwoordiger van de lokale politie bedoeld in artikel 3, kan, na goedkeuring bij consensus door alle effectief deelnemende leden van het LIVC R, een terugkoppelingsfiche van een persoon van wie het geval ter bespreking wordt voorgelegd in een LIVC R overeenkomstig artikel 3, § 2, meedelen aan de vertegenwoordigers van de diensten bedoeld in artikel 44/11/3ter, § 1, van de wet van 5 augustus 1992 op het politieambt die bevoegd zijn voor de geografisch zone van het betrokken LIVC R. De terugkoppelingsfiche bevat een evaluatie van de opvolging binnen het LIVC R. De terugkoppelingsfiche bevat geen tijdens het overleg meegedeelde geheimen.

§ 3. De verwerking van persoonsgegevens van de personen voorgedragen in een LIVC R overeenkomstig artikel 3, § 2, wordt niet toegestaan, behoudens de uitzonderingen door de wet bepaald.

Art. 4.

§ 1. De korpschef en/of de door hem aangestelde vertegenwoordiger van de lokale politie bedoeld in artikel 2, 17°, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.") en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt, van de personen van wie het geval ter bespreking wordt voorgelegd in een LIVC R overeenkomstig artikel 3, § 2, meedelen aan de leden van het LIVC R.

§ 2. De korpschef en/of de door hem aangestelde vertegenwoordiger van de lokale politie bedoeld in artikel 3, kan, na goedkeuring bij consensus door alle effectief deelnemende leden van het LIVC R, een terugkoppelingsfiche van een persoon van wie het geval ter bespreking wordt voorgelegd in een LIVC R overeenkomstig artikel 3, § 2, meedelen aan de vertegenwoordigers van de diensten bedoeld in artikel 2, 2° en 22°, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.") en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt die bevoegd zijn voor de geografisch zone van het betrokken LIVC R.

De terugkoppelingsfiche bevat een evaluatie van de opvolging binnen het LIVC R. De terugkoppelingsfiche bevat geen tijdens het overleg meegedeelde geheimen.

§ 3. De verwerking van persoonsgegevens van de personen voorgedragen in een LIVC R overeenkomstig artikel 3, § 2, wordt niet toegestaan, behoudens de uitzonderingen door de wet bepaald.

Afdeling 3 – Wijzigingsbepalingen van de wet van 5 augustus 1992 op het politieambt

Art. 44/2.

§ 1. Wanneer de uitoefening van de opdrachten van bestuurlijke politie en van gerechtelijke politie vereist dat de politiediensten de persoonsgegevens en de informatie bedoeld in artikel 44/1 structureren zodat ze rechtstreeks kunnen worden teruggevonden, worden deze verwerkt in een operationele politionele gegevensbank die behoort tot een van de in het tweede lid bedoelde categorieën van gegevensbanken volgens de eigen doelstellingen van elke categorie van gegevensbanken.

De categorieën van operationele politionele gegevensbanken zijn :

1° de Algemene Nationale Gegevensbank, hierna "A.N.G." genoemd;

2° de basisgegevensbanken;

3° de bijzondere gegevensbanken.

De in het eerste lid bedoelde doelstellingen worden respectievelijk nader bepaald in de artikelen 44/7, 44/11/2, § 1 en 44/11/3, § 2.]¹

§ 2. Wanneer de gezamenlijke uitoefening door alle of een deel van de overheden, organen, organismen, diensten, directies of de commissie bedoeld in artikel 44/11/3ter, elk binnen het kader van hun wettelijke bevoegdheden, van de opdrachten ter

Art. 44/2.

§ 1. Wanneer de uitoefening van de opdrachten van bestuurlijke politie en van gerechtelijke politie vereist dat de politiediensten de persoonsgegevens en de informatie bedoeld in artikel 44/1 structureren zodat ze rechtstreeks kunnen worden teruggevonden, worden deze verwerkt in een operationele politionele gegevensbank die behoort tot een van de in het tweede lid bedoelde categorieën van gegevensbanken volgens de eigen doelstellingen van elke categorie van gegevensbanken.

De categorieën van operationele politionele gegevensbanken zijn :

1° de Algemene Nationale Gegevensbank, hierna "A.N.G." genoemd;

2° de basisgegevensbanken;

3° de bijzondere gegevensbanken.

De in het eerste lid bedoelde doelstellingen worden respectievelijk nader bepaald in de artikelen 44/7, 44/11/2, § 1 en 44/11/3, § 2.]¹

§ 2. [...]

§ 3. Wanneer in de uitvoering van de opdrachten van bestuurlijke en gerechtelijke politie, technische hulpmiddelen worden gebruikt om automatisch persoonsgegevens

voorkoming en ter opvolging van het terrorisme in de zin van artikel 8, 1°, b) van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, of het extremisme in de zin van artikel 8, 1°, c) van dezelfde wet wanneer dat tot terrorisme kan leiden, vereist dat deze de persoonsgegevens en de informatie met betrekking tot deze opdrachten structureren zodat ze rechtstreeks kunnen worden teruggevonden, worden deze persoonsgegevens en informatie verwerkt in een of meerdere gemeenschappelijke gegevensbanken.

De voorwaarden van de oprichting van de gemeenschappelijke gegevensbanken en van de verwerking van persoonsgegevens en informatie in deze gegevensbanken worden bepaald in artikel 44/11/3bis.

Artikel 139, tweede lid, van het Strafwetboek is van toepassing op de gemeenschappelijke gegevensbanken.

§ 3. Wanneer in de uitvoering van de opdrachten van bestuurlijke en gerechtelijke politie, technische hulpmiddelen worden gebruikt om automatisch persoonsgegevens en informatie van technische aard te verzamelen, zodanig gestructureerd dat zij rechtstreeks kunnen worden teruggevonden, worden deze gegevens verwerkt in een technische gegevensbank.

Een technische gegevensbank wordt gecreëerd ingevolge het gebruik van :

1° intelligente camera's voor de automatische nummerplaatherkenning;

2° intelligente systemen voor de automatische nummerplaatherkenning.

Onder intelligente systemen voor de automatische nummerplaatherkenning wordt verstaan elke intelligente software die het mogelijk maakt om automatisch de door camera's geregistreerde beelden te verwerken, om de nummerplaatgegevens eruit te halen op basis van bepaalde vooropgestelde criteria.

en informatie van technische aard te verzamelen, zodanig gestructureerd dat zij rechtstreeks kunnen worden teruggevonden, worden deze gegevens verwerkt in een technische gegevensbank.

Een technische gegevensbank wordt gecreëerd ingevolge het gebruik van :

1° intelligente camera's voor de automatische nummerplaatherkenning;

2° intelligente systemen voor de automatische nummerplaatherkenning.

Onder intelligente systemen voor de automatische nummerplaatherkenning wordt verstaan elke intelligente software die het mogelijk maakt om automatisch de door camera's geregistreerde beelden te verwerken, om de nummerplaatgegevens eruit te halen op basis van bepaalde vooropgestelde criteria.

Een technische gegevensbank kan zowel op lokaal als op nationaal niveau gecreëerd worden.

De voorwaarden voor de oprichting van dit type van gegevensbank en de voorwaarden voor de verwerking van de persoonsgegevens en informatie die hierin worden bijgehouden worden verder bepaald in artikelen 44/11/3sexies tot 44/11/3decies.

Een technische gegevensbank kan zowel op lokaal als op nationaal niveau gecreëerd worden.

De voorwaarden voor de oprichting van dit type van gegevensbank en de voorwaarden voor de verwerking van de persoonsgegevens en informatie die hierin worden bijgehouden worden verder bepaald in artikelen 44/11/3sexies tot 44/11/3decies.

Art. 44/4.

§ 1. Voor de verwerking van persoonsgegevens en informatie bedoeld in artikel 44/1 met inbegrip van deze ingevoegd in de gegevensbanken bedoeld in artikel 44/2, § 1, tweede lid, 1° en 2°, is, voor wat betreft bestuurlijke politie, de verwerkingsverantwoordelijke de minister van Binnenlandse Zaken.

Voor de verwerking van persoonsgegevens en informatie bedoeld in artikel 44/1 met inbegrip van deze ingevoegd in de gegevensbanken bedoeld in artikel 44/2, § 1, tweede lid, 1° en 2°, is, voor wat betreft gerechtelijke politie, de verwerkingsverantwoordelijke de minister van Justitie.

Voor wat betreft de gegevensbanken bedoeld in artikel 44/2, § 1, tweede lid, 3°, zijn de verwerkingsverantwoordelijken de korpschefs, de commissaris-generaal, de directeurs-generaal of de directeurs die de doeleinden van en de middelen voor deze bijzondere gegevensbanken hebben bepaald.

§ 2. De ministers van Binnenlandse Zaken en van Justitie bepalen, elk binnen het kader van hun bevoegdheden en onverminderd de eigen bevoegdheden van de gerechtelijke overheden, bij dwingende richtlijn de maatregelen die nodig zijn om het beheer en de veiligheid, waaronder in het bijzonder de aspecten met betrekking tot de betrouwbaarheid, de vertrouwelijkheid, de beschikbaarheid, de traceerbaarheid en de integriteit van de persoonsgegevens en de informatie die worden verwerkt in de gegevensbanken bedoeld in artikel 44/2, te verzekeren.

Art. 44/4.

§ 1. Voor de verwerking van persoonsgegevens en informatie bedoeld in artikel 44/1 met inbegrip van deze ingevoegd in de gegevensbanken bedoeld in artikel 44/2, § 1, tweede lid, 1° en 2°, is, voor wat betreft bestuurlijke politie, de verwerkingsverantwoordelijke de minister van Binnenlandse Zaken.

Voor de verwerking van persoonsgegevens en informatie bedoeld in artikel 44/1 met inbegrip van deze ingevoegd in de gegevensbanken bedoeld in artikel 44/2, § 1, tweede lid, 1° en 2°, is, voor wat betreft gerechtelijke politie, de verwerkingsverantwoordelijke de minister van Justitie.

Voor wat betreft de gegevensbanken bedoeld in artikel 44/2, § 1, tweede lid, 3°, zijn de verwerkingsverantwoordelijken de korpschefs, de commissaris-generaal, de directeurs-generaal of de directeurs die de doeleinden van en de middelen voor deze bijzondere gegevensbanken hebben bepaald.

§ 2. De ministers van Binnenlandse Zaken en van Justitie bepalen, elk binnen het kader van hun bevoegdheden en onverminderd de eigen bevoegdheden van de gerechtelijke overheden, bij dwingende richtlijn de maatregelen die nodig zijn om het beheer en de veiligheid, waaronder in het bijzonder de aspecten met betrekking tot de betrouwbaarheid, de vertrouwelijkheid, de beschikbaarheid, de traceerbaarheid en de integriteit van de persoonsgegevens en de informatie die worden verwerkt in de gegevensbanken bedoeld in artikel 44/2, te verzekeren.

De logbestanden worden op zijn minst voor de volgende verwerkingen in de in artikel 44/2 bedoelde gegevensbanken aangemaakt: de verzameling, de wijziging, de raadpleging, de mededeling, met inbegrip van de doorgiften, de archivering, de koppeling en de uitwissing.

De logbestanden van de raadpleging en de mededeling laten toe om:

1° de beweegreden, de datum en het tijdstip van die verwerkingen vast te stellen;

2° vast te stellen welke categorieën van personen de persoonsgegevens hebben geraadpleegd alsook de persoon die die gegevens heeft geraadpleegd te identificeren;

3° vast te stellen welke systemen die gegevens hebben meegedeeld;

4° de categorieën van ontvangers van de persoonsgegevens vast te stellen en indien mogelijk de identiteit van de ontvangers van die gegevens.

De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, na advies van het Controleorgaan, andere types verwerkingen vastleggen waarvoor de logbestanden worden aangemaakt.

Er worden gepaste maatregelen getroffen om de veiligheid van de logbestanden te verzekeren, in het bijzonder om elke niet-toegelaten verwerking te beletten en de integriteit van de verwerkte gegevens te verzekeren.

De procedures voor de toegang tot de logbestanden waarborgen de noodzaak en de proportionaliteit van de toegang tot de logginggegevens om de in artikel 56, § 2, van de wet gegevensbescherming bedoelde doeleinden te bereiken.

Die procedures worden voor advies voorgelegd aan het Controleorgaan.

De korpschefs voor de lokale politie en de commissaris-generaal, de directeurs-generaal en de directeurs voor de federale

De logbestanden worden op zijn minst voor de volgende verwerkingen in de in artikel 44/2 bedoelde gegevensbanken aangemaakt: de verzameling, de wijziging, de raadpleging, de mededeling, met inbegrip van de doorgiften, de archivering, de koppeling en de uitwissing.

De logbestanden van de raadpleging en de mededeling laten toe om:

1° de beweegreden, de datum en het tijdstip van die verwerkingen vast te stellen;

2° vast te stellen welke categorieën van personen de persoonsgegevens hebben geraadpleegd alsook de persoon die die gegevens heeft geraadpleegd te identificeren;

3° vast te stellen welke systemen die gegevens hebben meegedeeld;

4° de categorieën van ontvangers van de persoonsgegevens vast te stellen en indien mogelijk de identiteit van de ontvangers van die gegevens.

De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, na advies van het Controleorgaan, andere types verwerkingen vastleggen waarvoor de logbestanden worden aangemaakt.

Er worden gepaste maatregelen getroffen om de veiligheid van de logbestanden te verzekeren, in het bijzonder om elke niet-toegelaten verwerking te beletten en de integriteit van de verwerkte gegevens te verzekeren.

De procedures voor de toegang tot de logbestanden waarborgen de noodzaak en de proportionaliteit van de toegang tot de logginggegevens om de in artikel 56, § 2, van de wet gegevensbescherming bedoelde doeleinden te bereiken.

Die procedures worden voor advies voorgelegd aan het Controleorgaan.

De korpschefs voor de lokale politie en de commissaris-generaal, de directeurs-generaal en de directeurs voor de federale

politie staan borg voor de goede uitvoering van deze richtlijnen voor wat de gegevensbanken bedoeld in artikel 44/2, §§ 1 en 3, betreft.

De beheerder, aangewezen in rechte of in feite waarborgt de goede uitvoering van deze richtlijnen voor wat de gegevensbanken bedoeld in artikel 44/2, § 2, betreft.

§ 3. Onverminderd de bevoegdheden van de gerechtelijke overheden, bepalen de ministers van Binnenlandse Zaken en van Justitie, elk binnen het kader van hun bevoegdheden, bij algemene en bindende richtlijn, gepubliceerd in het Belgisch Staatsblad de toegangsregels voor de leden van de politiediensten tot de gegevensbanken bedoeld in artikel 44/2, §§ 1 en 3.

§ 4. De ministers van Binnenlandse Zaken en van Justitie bepalen, elk binnen het kader van hun bevoegdheden, bij algemene en bindende richtlijn, gepubliceerd in het Belgisch Staatsblad de nadere regels betreffende de koppeling van de gegevensbanken bedoeld in artikel 44/2 onderling of met andere gegevensbanken waartoe de politiediensten toegang hebben door of krachtens de wet of internationale verdragen die België binden.

Deze richtlijnen bepalen minstens op basis van de toereikende, terzake dienende en niet overmatige aard, de categorieën van gegevensbanken die onderling kunnen worden verbonden, de nadere regels betreffende de koppeling en de toegangsregels van de leden van de politiediensten betreffende het bestaan van relevante informatie in deze onderling gekoppelde gegevensbanken of, in voorkomend geval, betreffende de gegevens zelf, alsmede tot de daaruit voortvloeiende verwerkingen.

§ 5. De in de §§ 3 en 4 bedoelde profielen en nadere regels voor de toegang worden bepaald, onder andere op basis:

1° van de nood er kennis van te nemen, met inbegrip van de noodzaak de verwerkte gegevens te kruisen of te coördineren;

politie staan borg voor de goede uitvoering van deze richtlijnen voor wat de gegevensbanken bedoeld in artikel 44/2, §§ 1 en 3, betreft.

[...]

§ 3. Onverminderd de bevoegdheden van de gerechtelijke overheden, bepalen de ministers van Binnenlandse Zaken en van Justitie, elk binnen het kader van hun bevoegdheden, bij algemene en bindende richtlijn, gepubliceerd in het Belgisch Staatsblad de toegangsregels voor de leden van de politiediensten tot de gegevensbanken bedoeld in artikel 44/2, §§ 1 en 3.

§ 4. De ministers van Binnenlandse Zaken en van Justitie bepalen, elk binnen het kader van hun bevoegdheden, bij algemene en bindende richtlijn, gepubliceerd in het Belgisch Staatsblad de nadere regels betreffende de koppeling van de gegevensbanken bedoeld in artikel 44/2 onderling of met andere gegevensbanken waartoe de politiediensten toegang hebben door of krachtens de wet of internationale verdragen die België binden.

Deze richtlijnen bepalen minstens op basis van de toereikende, terzake dienende en niet overmatige aard, de categorieën van gegevensbanken die onderling kunnen worden verbonden, de nadere regels betreffende de koppeling en de toegangsregels van de leden van de politiediensten betreffende het bestaan van relevante informatie in deze onderling gekoppelde gegevensbanken of, in voorkomend geval, betreffende de gegevens zelf, alsmede tot de daaruit voortvloeiende verwerkingen.

§ 5. De in de §§ 3 en 4 bedoelde profielen en nadere regels voor de toegang worden bepaald, onder andere op basis:

1° van de nood er kennis van te nemen, met inbegrip van de noodzaak de verwerkte gegevens te kruisen of te coördineren;

2° van de wettelijke doeleinden van elke gegevensbank;

3° van de verschillende categorieën van de in artikel 44/5 bedoelde personen;

4° van de evaluatie van de gegevens;

5° van de validatiestatus van de verwerkte gegevens.

De in de §§ 3 en 4 bedoelde toegangen moeten, oorspronkelijk of standaard, zo ontworpen worden dat de geëvalueerde en gevalideerde gegevens duidelijk zichtbaar zijn en prioritair kunnen worden geëxploiteerd.

De toegangsprofielen en de identificatie van personen die toegang hebben, worden ter beschikking gesteld van het Controleorgaan.

§ 6. De ministers van Binnenlandse Zaken en van Justitie bepalen, elk binnen het kader van hun bevoegdheden, bij algemene en bindende richtlijn gepubliceerd in het Belgisch Staatsblad, de toereikende, terzake dienende en niet overmatige maatregelen met betrekking tot de koppeling of correlatie van de technische gegevensbanken bedoeld in artikel 44/2, § 3, met de gegevensbanken bedoeld in artikel 44/2, §§ 1 en 2, of met andere gegevensbanken waartoe de politiediensten toegang hebben door of krachtens de wet of internationale verdragen die België binden.

Deze richtlijn houdt rekening met criteria inzake tijd, ruimte en frequentie van de koppelingen en correlaties. Zij wijst minstens de overheid aan die dit soort maatregelen toestaat, alsook de gegevensbanken die onderling kunnen worden verbonden.

Onderafdeling 7bis. - De gemeenschappelijke gegevensbanken.

2° van de wettelijke doeleinden van elke gegevensbank;

3° van de verschillende categorieën van de in artikel 44/5 bedoelde personen;

4° van de evaluatie van de gegevens;

5° van de validatiestatus van de verwerkte gegevens.

De in de §§ 3 en 4 bedoelde toegangen moeten, oorspronkelijk of standaard, zo ontworpen worden dat de geëvalueerde en gevalideerde gegevens duidelijk zichtbaar zijn en prioritair kunnen worden geëxploiteerd.

De toegangsprofielen en de identificatie van personen die toegang hebben, worden ter beschikking gesteld van het Controleorgaan.

§ 6. De ministers van Binnenlandse Zaken en van Justitie bepalen, elk binnen het kader van hun bevoegdheden, bij algemene en bindende richtlijn gepubliceerd in het Belgisch Staatsblad, de toereikende, terzake dienende en niet overmatige maatregelen met betrekking tot de koppeling of correlatie van de technische gegevensbanken bedoeld in artikel 44/2, § 3, met de gegevensbanken bedoeld in artikel 44/2, §§ 1 en 2, of met andere gegevensbanken waartoe de politiediensten toegang hebben door of krachtens de wet of internationale verdragen die België binden.

Deze richtlijn houdt rekening met criteria inzake tijd, ruimte en frequentie van de koppelingen en correlaties. Zij wijst minstens de overheid aan die dit soort maatregelen toestaat, alsook de gegevensbanken die onderling kunnen worden verbonden.

Onderafdeling 7bis. - De gemeenschappelijke gegevensbanken.

Opgeheven

Art. 44/11/3bis.

§ 1. Voor de gezamenlijke uitoefening van de opdrachten bedoeld in artikel 44/2, § 2, kunnen de ministers van Binnenlandse Zaken en van Justitie gezamenlijk gemeenschappelijke gegevensbanken oprichten waarvan zij de verantwoordelijken voor de verwerking worden.

§ 2. De oprichting van een gemeenschappelijke gegevensbank wordt gemotiveerd door een van de volgende doeleinden :

1° de strategische, tactische of operationele noodzaak om gezamenlijk persoonsgegevens en informatie te verwerken voor het uitoefenen van de respectievelijke bevoegdheden van de overheden, organen, organismen, diensten, directies of de commissie bedoeld in artikel 44/2, § 2;

2° de hulp bij het nemen van beslissingen door de bestuurlijke overheden of de overheden van bestuurlijke politie of van gerechtelijke politie.

§ 3. Voorafgaand aan haar oprichting, doen de ministers van Binnenlandse Zaken en van Justitie aangifte van de gemeenschappelijke gegevensbank alsook van de verwerkingsmodaliteiten, waaronder deze met betrekking tot de registratie van de gegevens en van de verschillende categorieën en types van persoonsgegevens en informatie die verwerkt worden bij het Comité en het Controleorgaan bedoeld in artikel 44/11/3quinquies/2, die gezamenlijk een advies uitbrengen binnen de 30 dagen vanaf de ontvangst van de aangifte.

§ 4. De gemeenschappelijke gegevensbanken maken de verwerking van verschillende categorieën van persoonsgegevens mogelijk onder meer met betrekking tot personen, groeperingen, organisaties en fenomenen die toereikend, ter zake dienend en niet overmatig zijn in verhouding tot de opdrachten bedoeld in artikel 44/2, § 2, en de doeleinden bedoeld in § 2.

Art. 44/11/3bis.

Opgeheven

Voor elke gemeenschappelijke gegevensbank bepaalt, na advies van het Comité en het Controleorgaan bedoeld in artikel 44/11/3quinquies/2, een koninklijk besluit vastgesteld na overleg in de Ministerraad de types van verwerkte persoonsgegevens, de regels op het gebied van de verantwoordelijkheden op het vlak van de bescherming van de persoonlijke levenssfeer van de organen, diensten, overheden en organismen die gegevens verwerken, de regels op het gebied van de veiligheid van de verwerkingen, de regels van het gebruik, de bewaring en de uitwissing van de gegevens.

§ 5. Onverminderd de archiefwet van 24 juni 1955, worden de in de gemeenschappelijke gegevensbanken bewaarde persoonsgegevens uitgewist vanaf het ogenblik dat de doeleinden bedoeld in § 2 verdwijnen, en ten laatste 30 jaar na de laatste verwerking.

Na de laatste verwerking wordt er minimaal om de drie jaar onderzocht of de persoonsgegevens nog steeds een rechtstreeks verband houden met een van de doeleinden van § 2. Indien dit niet het geval is, worden de gegevens uitgewist.

§ 6. Alle door de directies, diensten, organen, organismen, overheden of de commissie uitgevoerde verwerkingen in de gemeenschappelijke gegevensbanken maken het voorwerp uit van een oplijsting die bewaard wordt gedurende 30 jaar vanaf de in de gemeenschappelijke gegevensbanken uitgevoerde verwerking.

§ 7. De persoonsgegevens en de informatie die uitgewist moeten worden, kunnen gearchiveerd worden gedurende een termijn van maximum 30 jaar.

Na afloop van deze termijn, worden deze gegevens en informatie uitgewist onverminderd de archiefwet van 24 juni 1955.

De raadpleging van de archieven van een gemeenschappelijke gegevensbank mag slechts gebeuren in het kader van de volgende doeleinden :

1° de ondersteuning bij het bepalen en het uitwerken van het politie- en veiligheidsbeleid inzake terrorisme en extremisme dat tot terrorisme kan leiden;

2° de verwerking van de antecedenten in het kader van onderzoek met betrekking tot een terrorismemisdad;

3° de verdediging in rechte van de overheden bedoeld in artikel 44/11/3bis, § 2, 2°.

Het resultaat van de exploitatie van de archieven van de gemeenschappelijke gegevensbank voor het in het eerste lid, 1°, bedoelde doeleinde is geanonimiseerd.

§ 8. Bijkomende nadere beheersregels van de gemeenschappelijke gegevensbanken kunnen bepaald worden door een koninklijk besluit vastgesteld na overleg in de Ministerraad, na advies van het Comité en het Controleorgaan bedoeld in artikel 44/11/3quinquies/2.

§ 9. Voor elke gemeenschappelijke gegevensbank wordt op gezamenlijk voorstel van de ministers van Binnenlandse Zaken en van Justitie door de Koning een beheerder aangewezen. Deze beheerder is belast met het technisch en functioneel beheer van de gemeenschappelijke gegevensbank.

De beheerder verzekert minstens de volgende opdrachten :

- het creëren en het ter beschikking stellen van de gemeenschappelijke gegevensbank door een beroep te doen op de noodzakelijke technische middelen op basis van de mogelijkheden die voortvloeien uit de ICT-omgeving eigen aan zijn dienst;
- het beheren van de gemeenschappelijke gegevensbank en er het onderhoud van verzekeren;
- het in functionele regels vertalen van de door de ministers krachtens § 3 aangegeven nadere regels met betrekking tot de verwerking van de informatie;

- de technische normen bepalen en doen toepassen die noodzakelijk zijn voor de werking van de gemeenschappelijke gegevensbank;

- een advies op technisch en/of functioneel vlak verstrekken op vraag van de operationeel verantwoordelijke of van [2 de functionaris voor gegevensbescherming bedoeld in artikel 44/11/3quinquies/1]2;

- de rechten en de toegangen organiseren tot de in de gemeenschappelijke gegevensbank te voeren verwerkingen;

- een documentatie en een technische ondersteuning aanbieden;

- het zowel op technisch als op functioneel vlak beheren en behandelen van de rapportering van de veiligheidsincidenten.

§ 10. Voor elke gemeenschappelijke gegevensbank wordt op gezamenlijk voorstel van de ministers van Binnenlandse Zaken en van Justitie een operationeel verantwoordelijke door de Koning aangewezen. Deze verantwoordelijke is belast met het operationeel beheer van de gemeenschappelijke gegevensbank.

De operationeel verantwoordelijke verzekert minstens de volgende opdrachten :

- het controleren van de kwaliteit van de in de gemeenschappelijke gegevensbank verwerkte gegevens en zich verzekeren van de relevantie ervan in verhouding tot de doeleinden waarvoor de gegevensbank opgericht werd;

- een coördinatiefunctie uitoefenen voor de voeding van de gemeenschappelijke gegevensbank door de verschillende diensten;

- het organiseren van de passende samenwerking tussen de partnerdiensten met het oog op de verwezenlijking van de voorziene doeleinden;

- er op toe zien dat de exploitatie van de persoonsgegevens en de informatie

beantwoordt aan de in § 2, beschreven doeleinden.

§ 11. Voor elke gemeenschappelijke gegevensbank, kunnen bijzondere opdrachten van de beheerder en van de operationeel verantwoordelijke bepaald worden door de Koning.

Art. 44/11/3ter.

Art. 44/11/3ter.

§ 1. Op basis van de behoefte om te kennen, zijn alle of een gedeelte van de persoonsgegevens en informatie van de gemeenschappelijke gegevensbanken rechtstreeks toegankelijk voor het Orgaan en de volgende diensten die belast zijn met bevoegdheden in de materies bedoeld in artikel 44/2, § 2 :

Opgeheven

- a) het Coördinatieorgaan voor de dreigingsanalyse;
- b) de geïntegreerde politie;
- c) de inlichtingen- en veiligheidsdiensten.

In het kader van de uitoefening van hun opdrachten bedoeld in artikel 44/11/3quinquies/2 zijn het geheel of een deel van de persoonsgegevens en informatie van de gemeenschappelijke gegevensbanken rechtstreeks toegankelijk voor het Comité en het Controleorgaan bedoeld in artikel 44/11/3quinquies/2.

§ 2. Op basis van de behoefte om te kennen, onder meer op strategisch, tactisch of operationeel vlak, kunnen de persoonsgegevens en de informatie van de gemeenschappelijke gegevensbanken meegedeeld worden aan of rechtstreeks toegankelijk zijn voor de volgende diensten of het voorwerp uitmaken van een rechtstreekse bevraging door deze diensten wanneer zij belast zijn met bevoegdheden in de domeinen die voorzien zijn in artikel 44/2, § 2 :

- a) de Vaste Commissie voor de lokale politie;
- b) de Algemene Directie Crisiscentrum;

c) de Algemene Directie Veiligheid en Preventie van de Federale overheidsdienst Binnenlandse Zaken;

d) het directoraat-generaal Penitentiare Inrichtingen en de penitentiare inrichtingen;

e) de Federale overheidsdienst Buitenlandse Zaken, Directoraat-generaal Consulaire Zaken;

f) het Openbaar Ministerie;

g) de Cel voor Financiële Informatieverwerking;

h) de Dienst Vreemdelingenzaken;

i) de onderzoeks- en opsporingsdiensten van de Algemene Administratie der douane en accijnzen.

De Koning bepaalt bij een besluit vastgesteld na overleg in de Ministerraad, na advies van het Comité en het Controleorgaan bedoeld in artikel 44/11/3quinquies/2, het type toegang en de nadere regels ervan voor de organen, overheden, directies of diensten bedoeld in het eerste lid.

§ 3. De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, na advies van het Comité en het Controleorgaan bedoeld in artikel 44/11/3quinquies/2 andere Belgische openbare overheden, andere openbare organen of organismen of andere organen of organismen van openbaar nut aanwijzen die door de wet belast zijn met de toepassing van de strafwet of die wettelijke opdrachten van openbare veiligheid hebben, die, wanneer zij belast zijn met bevoegdheden in de domeinen die voorzien zijn in artikel 44/2, § 2, op basis van de behoefte om te kennen, onder meer op strategisch, tactisch of operationeel vlak een toegang kunnen hebben tot de gemeenschappelijke gegevensbanken.

De Koning bepaalt bij een besluit vastgesteld na overleg in de Ministerraad, na advies van het Comité en het Controleorgaan bedoeld in artikel

44/11/3quinquies/2, het type toegang en de nadere regels ervan voor de organen, overheden, directies of diensten bedoeld in het eerste lid.

Bovendien wijzen de ministers van Binnenlandse Zaken en van Justitie gezamenlijk, op basis van de behoefte om te kennen, onder meer op strategisch, tactisch of operationeel vlak, de organen, overheden of organismen bedoeld in het eerste lid aan aan welke de uit de gemeenschappelijke gegevensbanken voortkomende persoonsgegevens en informatie kunnen meegedeeld worden.

Deze organen, overheden of organismen worden bepaald in de voorafgaande aangifte bedoeld in artikel 44/11/3bis, § 3.

§ 4. Het Orgaan en de diensten bedoeld in § 1 alsook de directies, diensten, organen, organismen, overheden of commissie bedoeld in §§ 2 en 3 die rechtstreeks toegang hebben tot de gemeenschappelijke gegevensbanken zenden ambtshalve de in artikel 44/2, § 2, bedoelde persoonsgegevens en informatie aan de gemeenschappelijke gegevensbanken toe. Deze persoonsgegevens en informatie worden onder hun verantwoordelijkheid en volgens hun interne validatieprocedures opgenomen in de gemeenschappelijke gegevensbanken overeenkomstig de nadere regels die worden bepaald door de Koning, na het advies bedoeld in artikel 44/11/3bis, § 3 te hebben ontvangen.

De persoonsgegevens en informatie ingevoerd in de gemeenschappelijke gegevensbanken worden onverwijld meegedeeld aan de korpschef van elke betrokken politiezone. Met naleving van de voorwaarden bepaald in en met toepassing van artikel 44/1, § 4, informeert hij de bevoegde bestuurlijke politieoverheden.

§ 5. In afwijking van § 4, wordt de verplichting tot voeding van de gemeenschappelijke gegevensbanken uitgesteld wanneer en zolang de bevoegde magistraat, met instemming van de federale procureur, meent dat deze voeding de uitoefening van de strafvordering of de veiligheid van een persoon in het gedrang

kan brengen. In voorkomend geval kan de federale procureur de nadere regels voor deze afwijking bepalen. De federale procureur gaat op regelmatige tijdstippen de noodzaak tot behoud van het uitstel van de voeding van de gemeenschappelijke gegevensbanken na.

In afwijking van § 4, wordt de verplichting tot voeding van de gemeenschappelijke gegevensbanken uitgesteld wanneer en zolang de leidinggevende van een inlichtingen- en veiligheidsdienst oordeelt dat de deze voeding de veiligheid van een persoon in gevaar kan brengen of wanneer de informatie afkomstig is van een buitenlandse dienst die uitdrukkelijk gevraagd heeft deze niet aan andere diensten toe te zenden.

Art. 44/11/3quater.

Met als doel het voorkomen en het bestrijden van het terrorisme en het extremisme dat tot terrorisme kan leiden, te versterken, kunnen de van een gemeenschappelijke gegevensbank afkomstige persoonsgegevens en informatie volgens de door de Koning bepaalde nadere regels, na evaluatie door de beheerder, de operationeel verantwoordelijke, het Orgaan en de diensten bedoeld in artikel 44/11/3ter, § 1, meegedeeld worden aan een derde overheid of een derde eenheid.

Art. 44/11/3quater.

Opgeheven

Art. 44/11/3quinquies.

Voor de doeleinden bedoeld in artikel 44/2, § 2, en onverminderd de internationale rechtsregels die België verbinden, kunnen de persoonsgegevens en de informatie van de gemeenschappelijke gegevensbanken in overeenstemming met artikel 44/11/13 meegedeeld worden aan buitenlandse politiediensten, aan de internationale organisaties voor gerechtelijke en politionele samenwerking en aan de internationale rechtshandhavingdiensten.

Voor de doeleinden bedoeld in artikel 44/2, § 2, en onverminderd de internationale

Art. 44/11/3quinquies.

Opgeheven

rechtsregels die België verbinden, kunnen de persoonsgegevens en de informatie van de gemeenschappelijke gegevensbanken in overeenstemming met de artikelen 21 en 22 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, meegedeeld worden aan de buitenlandse inlichtingendiensten en aan de organen die belast zijn met de analyse van de dreiging of hun gelijken.

De Koning bepaalt de nadere regels van de mededeling bedoeld in het eerste en het tweede lid.

Art. 44/11/3quinquies/1.

Een functionaris voor gegevensbescherming wordt gezamenlijk door de ministers van Binnenlandse Zaken en van Justitie aangewezen voor de persoonsgegevens en de informatie die verwerkt worden in het kader van de gemeenschappelijke gegevensbanken bedoeld in artikel 44/2, § 2.

Opgeheven

Aanvullend op de in de wet gegevensbescherming voorziene opdrachten wordt de functionaris voor gegevensbescherming belast met de volgende opdrachten:

1° het verstrekken van deskundige adviezen inzake informatieveiligheid, inzake bescherming van gegevens en informatie en inzake hun verwerking en in het bijzonder waakt hij over de eerbiediging van de algemene voorwaarden voor de rechtmatigheid van de verwerking met betrekking tot verwerkingen van persoonsgegevens;

2° het toepassen, het bijwerken en het controleren van een beleid inzake beveiliging en bescherming van gegevens;

3° het uitvoeren van andere opdrachten inzake bescherming van gegevens en de beveiliging die bepaald worden door de Koning of die hem door de ministers van Binnenlandse Zaken en Justitie worden toevertrouwd.

Art. 44/11/3quinquies/1.

Hij oefent zijn functie uit, volledig onafhankelijk van de overheden, organen, instellingen, diensten en directies bedoeld in artikel 44/11/3ter. Hij brengt rechtstreeks verslag uit bij de ministers van Binnenlandse Zaken en Justitie.

Art. 44/11/3quinquies/2.

Met eerbied voor de uitoefening van hun respectievelijke bevoegdheden, wordt de controle op de verwerking van de in de gegevensbanken bedoeld in artikel 44/2, § 2, vervatte informatie en persoonsgegevens gezamenlijk verzekerd door:

1° het Controleorgaan;

2° het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, bedoeld in artikel 28 van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse.

Zij kunnen op elk moment de aanbevelingen uitvaardigen die zij noodzakelijk achten voor de in de gemeenschappelijke gegevensbanken uitgevoerde verwerkingen.

Art. 44/11/3quinquies/2.

Opgeheven

Art. 44/11/9bis (nieuw)

Wanneer de leden van de politiediensten in het kader van hun opdrachten van bestuurlijke of gerechtelijke politie moeten samenwerken met de gezondheids-, hulp- en/of reddingsdiensten, kunnen zij persoonsgegevens en informatie meedelen voor zover deze toereikend, ter zake dienend en strikt noodzakelijk zijn om de leden van de gezondheids-, hulp- en/of reddingsdiensten in staat te stellen hun taken in optimale veiligheidsomstandigheden uit te voeren en om de veiligheid en de psychische en fysieke integriteit te waarborgen van eenieder bij de uitvoering van die taken.

Afdeling 4 – Wijzigingsbepalingen van de Consulair Wetboek

Art. 39/4

De weigering van afgifte, van een Belgische identiteitskaart wordt opgeheven:

1° in de gevallen bedoeld in artikel 39/2, § 1, 1°, zodra de vrijheidsbeperkende gerechtelijke maatregel een einde neemt;

2° in het geval bedoeld in artikel 39/2, § 1, 2°, na een beslissing tot seponering van het openbaar ministerie, een buitenvervolginstelling of een eindbeslissing, door het onderzoeksgerecht zetelend als vonnisgerecht, of een vonnis of arrest in kracht van gewijsde ten aanzien van de betrokkene;

3° in het geval bedoeld in artikel 39/2, § 1, 3°, zodra de nationaliteit en de identiteit van de aanvrager wettelijk vaststaan;

4° in het geval bedoeld in artikel 39/2, § 2, zodra het daartoe bevoegde orgaan, de bevoegde dienst of het bevoegde organisme besluit dat de aanvrager klaarblijkelijk niet langer een aanzienlijk risico of een aanzienlijke bedreiging vormt voor de openbare orde of de openbare veiligheid.

Het openbaar ministerie meldt op eigen initiatief aan de minister de identiteit van de Belgen die vallen onder de categorieën bedoeld in de bepalingen onder 1° en 2°. De bevoegde Belgische organen, diensten en organismen melden op eigen initiatief aan de minister de identiteit van de Belgen die vallen onder de categorie bedoeld in de bepaling onder 4°.

In het geval bedoeld in de bepaling onder 1° kan de minister evenwel, indien de aanvrager betrokken was bij feiten die beantwoorden aan de criteria zoals bedoeld in het artikel 6, § 1, 1° of 1° /1, van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Terrorist Fighters, het bevoegde orgaan, de bevoegde dienst of het bevoegde organisme bedoeld in het artikel 39/2, § 2, consulteren

Art. 39/4

De weigering van afgifte, van een Belgische identiteitskaart wordt opgeheven:

1° in de gevallen bedoeld in artikel 39/2, § 1, 1°, zodra de vrijheidsbeperkende gerechtelijke maatregel een einde neemt;

2° in het geval bedoeld in artikel 39/2, § 1, 2°, na een beslissing tot seponering van het openbaar ministerie, een buitenvervolginstelling of een eindbeslissing, door het onderzoeksgerecht zetelend als vonnisgerecht, of een vonnis of arrest in kracht van gewijsde ten aanzien van de betrokkene;

3° in het geval bedoeld in artikel 39/2, § 1, 3°, zodra de nationaliteit en de identiteit van de aanvrager wettelijk vaststaan;

4° in het geval bedoeld in artikel 39/2, § 2, zodra het daartoe bevoegde orgaan, de bevoegde dienst of het bevoegde organisme besluit dat de aanvrager klaarblijkelijk niet langer een aanzienlijk risico of een aanzienlijke bedreiging vormt voor de openbare orde of de openbare veiligheid.

Het openbaar ministerie meldt op eigen initiatief aan de minister de identiteit van de Belgen die vallen onder de categorieën bedoeld in de bepalingen onder 1° en 2°. De bevoegde Belgische organen, diensten en organismen melden op eigen initiatief aan de minister de identiteit van de Belgen die vallen onder de categorie bedoeld in de bepaling onder 4°.

In het geval bedoeld in de bepaling onder 1° kan de minister evenwel, indien de aanvrager betrokken was bij feiten die beantwoorden aan de criteria zoals bedoeld in **het artikel 2, 7° of 8°, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.") en tot wijziging van de wet van 30 juli 2018**

om na te gaan of de weigering van afgifte van een Belgische identiteitskaart niet behouden moet worden op basis van het artikel 39/2, § 2.

betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt, het bevoegde orgaan, de bevoegde dienst of het bevoegde organisme bedoeld in het artikel 39/2, § 2, consulteren om na te gaan of de weigering van afgifte van een Belgische identiteitskaart niet behouden moet worden op basis van het artikel 39/2, § 2.

Art. 65/1

De weigering van afgifte, van een Belgisch paspoort of reisdocument wordt opgeheven:

1° in de gevallen bedoeld in artikel 63, § 1, 1°, zodra de vrijheidsbeperkende gerechtelijke maatregel een einde neemt;

2° in het geval bedoeld in artikel 63, § 1, 2°, na een beslissing tot seponering van het openbaar ministerie, een buitenvervolginstelling of een eindbeslissing, door het onderzoeksgerecht zetelend als vonnisgerecht, of een vonnis of arrest in kracht van gewijsde ten aanzien van de betrokkene;

3° in het geval bedoeld in artikel 63, § 1, 3°, zodra de nationaliteit en de identiteit van de aanvrager wettelijk vaststaan;

4° in het geval bedoeld in artikel 63, § 1, 4°, zodra, overeenkomstig artikel 374/1 van het Burgerlijk Wetboek, ofwel de beide ouders of de ouder die alleen het ouderlijk gezag over het minderjarig niet-ontvoogd kind uitoefent, respectievelijk hun toestemming geven of zijn toestemming geeft voor de afgifte van het paspoort of reisdocument aan het kind, ofwel de bevoegde rechter daarvoor de toelating geeft;

5° in het geval bedoeld in artikel 63, § 2, zodra het daartoe bevoegde orgaan, de bevoegde dienst of het bevoegde organisme concludeert dat de aanvrager klaarblijkelijk

Art. 65/1

De weigering van afgifte, van een Belgisch paspoort of reisdocument wordt opgeheven:

1° in de gevallen bedoeld in artikel 63, § 1, 1°, zodra de vrijheidsbeperkende gerechtelijke maatregel een einde neemt;

2° in het geval bedoeld in artikel 63, § 1, 2°, na een beslissing tot seponering van het openbaar ministerie, een buitenvervolginstelling of een eindbeslissing, door het onderzoeksgerecht zetelend als vonnisgerecht, of een vonnis of arrest in kracht van gewijsde ten aanzien van de betrokkene;

3° in het geval bedoeld in artikel 63, § 1, 3°, zodra de nationaliteit en de identiteit van de aanvrager wettelijk vaststaan;

4° in het geval bedoeld in artikel 63, § 1, 4°, zodra, overeenkomstig artikel 374/1 van het Burgerlijk Wetboek, ofwel de beide ouders of de ouder die alleen het ouderlijk gezag over het minderjarig niet-ontvoogd kind uitoefent, respectievelijk hun toestemming geven of zijn toestemming geeft voor de afgifte van het paspoort of reisdocument aan het kind, ofwel de bevoegde rechter daarvoor de toelating geeft;

5° in het geval bedoeld in artikel 63, § 2, zodra het daartoe bevoegde orgaan, de bevoegde dienst of het bevoegde organisme concludeert dat de aanvrager klaarblijkelijk

niet langer een aanzienlijk risico of een aanzienlijke bedreiging vormt voor de openbare orde of de openbare veiligheid.

Het openbaar ministerie meldt op eigen initiatief aan de minister de identiteit van de Belgen die vallen onder de categorieën bedoeld in de bepalingen onder 1° en 2°. De griffier van de familierechtbank meldt op eigen initiatief aan de minister de identiteit van de minderjarige Belgen die vallen onder de categorie bedoeld in de bepaling onder 4°, voor zover het gaat om een beslissing van de familierechtbank. De bevoegde Belgische organen, diensten en organismen melden op eigen initiatief aan de minister de identiteit van de Belgen die vallen onder de categorie bedoeld in de bepaling onder 5°.

In het geval bedoeld in de bepaling onder 1° kan de minister evenwel, indien de aanvrager betrokken was bij feiten die beantwoorden aan de criteria zoals bedoeld in het artikel 6, § 1, 1° of 1° /1, van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Terrorist Fighters, het bevoegde orgaan, de bevoegde dienst of het bevoegde organisme bedoeld in het artikel 63, § 2, consulteren om na te gaan of de weigering van afgifte van een Belgisch paspoort of reisdocument niet behouden moet worden op basis van het artikel 63, § 2.

niet langer een aanzienlijk risico of een aanzienlijke bedreiging vormt voor de openbare orde of de openbare veiligheid.

Het openbaar ministerie meldt op eigen initiatief aan de minister de identiteit van de Belgen die vallen onder de categorieën bedoeld in de bepalingen onder 1° en 2°. De griffier van de familierechtbank meldt op eigen initiatief aan de minister de identiteit van de minderjarige Belgen die vallen onder de categorie bedoeld in de bepaling onder 4°, voor zover het gaat om een beslissing van de familierechtbank. De bevoegde Belgische organen, diensten en organismen melden op eigen initiatief aan de minister de identiteit van de Belgen die vallen onder de categorie bedoeld in de bepaling onder 5°.

In het geval bedoeld in de bepaling onder 1° kan de minister evenwel, indien de aanvrager betrokken was bij feiten die beantwoorden aan de criteria zoals bedoeld in **het artikel 2, 7° of 8°, van de wet van [DATUM] tot oprichting van de gemeenschappelijke gegevensbank “Terrorisme, Extremisme, Radicaliseringsproces” (“T.E.R.”) en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt**, het bevoegde orgaan, de bevoegde dienst of het bevoegde organisme bedoeld in het artikel 63, § 2, consulteren om na te gaan of de weigering van afgifte van een Belgisch paspoort of reisdocument niet behouden moet worden op basis van het artikel 63, § 2.



Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 97/2023 du 16 juin 2023

Objet: demandes d'avis concernant

- 1) un avant-projet de loi portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (ci-après « T.E.R. ») et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police (CO-A-2023-144) et**
- 2) un projet d'arrêté royal relatif à la banque de données commune T.E.R. (CO-A-2023-145)**

Version originale

Le Centre de Connaissances de l'Autorité de protection des données (ci-après « l'Autorité »),
Présent.e.s : Mesdames Cédrine Morlière, Nathalie Raghenon et Griet Verhenneman et Messieurs Yves-Alexandre de Montjoye et Bart Preneel;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après « LCA »);

Vu l'article 25, alinéa 3, de la LCA selon lequel les décisions du Centre de Connaissances sont adoptées à la majorité des voix ;

Vu le règlement (UE) 2016/679 *du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (ci-après « RGPD »);

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après « LTD »);

Vu la demande d'avis du Vice-Premier ministre et ministre de la Justice et de la Mer du Nord, Monsieur Vincent Van Quickenborne (ci-après « le demandeur »), reçue le 13.04.2023 ;

Émet, le 16 juin 2023, l'avis suivant¹ :

I. Objet et contexte de la demande d'avis

1. Le demandeur a introduit auprès de l'Autorité une demande d'avis concernant un avant-projet de loi portant création de la banque de données commune T.E.R. (ci-après « la BDC ») et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police (ci-après, « le Projet de loi ») ainsi qu'un projet d'arrêté royal relatif à la BDC (ci-après, « le Projet d'AR »).
2. Il est précisé que seules les nouveautés sont explicitées et commentées dans l'exposé des motifs. En ce qui concerne les dispositions existantes, transférées sans modification de fond, il est renvoyé aux justifications qui sous-tendaient leur adoption figurant dans les travaux préparatoires de la loi du 27 avril 2016 relatif à des mesures complémentaires en matière de lutte contre le terrorisme² et aux rapports au Roi des AR d'exécution précités.
3. A l'occasion de l'introduction de sa demande d'avis, le fonctionnaire délégué a précisé que l'avis de l'APD était uniquement demandé au sujet de la participation des services, qui ne relèvent pas de la compétence du COC et du Comité R, « *au fonctionnement de la BDC* ». Par conséquent, même lorsque cela n'est pas expressément mentionné dans le présent avis, il y a lieu de considérer que les observations de l'Autorité ne sont à prendre en compte que « *pour autant que les traitements de données à caractère personnel prévus par une version modifiée de ces projets impliquent toujours des services autres que ceux relevant de la compétence du COC et du Comité R* ».

a) Concernant la BDC

4. Le projet de loi entend transposer les dispositions de la loi sur la fonction de police (ci-après « LFP ») relatives aux BDC³ dans une loi spécifique et y intégrer, pour reprendre les termes de l'exposé des motifs, « *un maximum d'éléments* » contenus, à ce jour, dans les arrêtés d'exécution.

¹ La liste des principales abréviations figure en annexe du présent avis

² DOC 54-1727/001 et suivants

³ Créées par l'AR du 21 juillet 2016 relatif à la BDC « Terrorist Fighters » et par l'AR du 23 avril 2018 relatif à la BDC « Propagandiste de haine »

5. L'art. 3 du projet de loi dispose que la BDC « *permet le traitement commun, par tout ou partie des services de base⁴ et des services partenaires⁵, des données à caractère personnel et des informations relatives aux missions de prévention et de suivi du terrorisme et de l'extrémisme, lorsqu'il peut mener au terrorisme (...)⁶, de ces services, chacun dans le cadre de ses compétences légales* ».
6. Par rapport à la situation actuelle, les projets entendent (1) supprimer les accès dont disposaient jusqu'à présent l'Autorité Nationale de sécurité et de la Commission permanente de la police locale (ci-après « la CPPL »), (2) mentionner (et *de facto* étendre) les droits d'accès du service des Cultes et de la Laïcité et l'administration de la Trésorerie - qui figuraient jusqu'à présent dans un AR - dans la loi, (3) étendre les accès du service des Douanes et accises et du Centre de Crise (mais, en ce qui concerne ce dernier, uniquement pour les détachés de la police et de la Sûreté de l'Etat (ci-après « la VSSE ») au sein de la BELPIU⁷ et de l'Unité ETIAS⁸) et (4) créer de nouveaux droits d'accès au profit des services d'Aide à la Jeunesse des Communautés française et germanophone.
7. Seuls les services de base auront la possibilité de « *créer une entité* » ou fiche d'information⁹ (d'initiative ou sur proposition d'un service partenaire) au sujet de laquelle, après validation par l'OCAM, tous les services de base et les services partenaires disposant d'un droit d'écriture¹⁰, communiqueront et enregistreront les données (non classifiées) dont ils disposent. Il est expressément prévu que ces fiches d'informations peuvent être communiquées à des destinataires « *non partenaires* » (par exemple le bourgmestre)¹¹.

⁴ A savoir l'OCAM, la police intégrée (ci-après « la GPI ») et les services de renseignement et de sécurité (art. 2, 2°). Le commentaire de l'article précise qu'« *il s'agit de services répressifs ou d'analyse qui travaillent directement en première ligne avec les entités et les finalités T.E.R. ou dont le travail d'analyse porte sur ces entités et, qui sont conséquemment susceptibles d'avoir le plus de données relatives à ces entités ou de détecter prioritairement une nouvelle entité T.E.R.* ».

⁵ A savoir les « unités opérationnelles » du Centre de Crise national du Service public fédéral Intérieur ; la Direction Générale Sécurité et Prévention du Service public fédéral Intérieur ; la Direction Générale des Etablissements Pénitentiaires du Service public fédéral Justice ; la Direction générale Affaires Consulaires du Service public fédéral Affaires étrangères ; le Ministère public ; la Cellule de Traitement des Informations Financières ; la Direction générale de l'Office des Etrangers du Service public fédéral Intérieur (ci-après « l'OE ») ; l'Administration générale des douanes et accises du Service public fédéral Finances ; le service des cultes et de la laïcité du Service public fédéral Justice ; l'Administration générale de la Trésorerie du Service public fédéral Finances ; dans le cadre de leurs missions légales d'accompagnement judiciaire et de la surveillance d'auteurs d'infractions, l'Administration générale des Maisons de Justice de la Communauté Française, le département Maison de Justice du Ministère de la Communauté Germanophone, l'Agence flamande pour la Justice et le Maintien, l'Administration générale de l'Aide à la Jeunesse de la Communauté Française, le service d'Aide à la Jeunesse de la Communauté germanophone et l'Agence flamande Grandir Opgroeien.

⁶ Au sens de l'article 8, 1° b) et c) de la loi du 30 novembre 1998 des services de renseignement et de sécurité

⁷ L'Unité belge d'information des passagers (Passenger Information Unit ou PIU) visée au chapitre 7 de la loi du 25 décembre 2016 relative au traitement des données des passagers

⁸ Également appelé BelENU, instituée par le Règlement UE 2018/1240

⁹ Notamment au sujet d'une personne physique

¹⁰ En vertu du projet d'AR, sur les 11 services partenaires énumérés par l'art. 2 du projet de loi, seuls la DG Sécurité et Prévention, la DG Affaires Consulaires et le Service des cultes et de la laïcité sont limités à une interrogation (de type hit/no hit) de la BDC. Tous les autres disposent d'un droit d'écriture.

¹¹ Art. 24 du projet de loi

8. Les données relatives à la santé (physique et mentale) et des données relatives à la dangerosité d'une personne enregistrées dans la BDC peuvent également être communiquées par les services de base aux professionnels des soins de santé¹².
9. Le projet prévoit également une possibilité d'interconnexion d'autres banques de données « opérationnelles » d'un service de base ou d'un service partenaire ou avec une source authentique (par exemple le Registre national ou la DIV), afin de permettre une alimentation automatisée de la BDC par les données de sources authentiques ou la détection de hits par le croisement automatisé des données de la BDC avec les banques de données opérationnelles des services de base et des services partenaires¹³.
10. L'art. 3 du projet de loi mentionne la création d'« une » BDC. A cet égard, l'Autorité relève que la mention, dans la loi, du caractère unique de la BDC est une nouveauté par rapport au libellé des textes qu'il entend remplacer¹⁴ et à la compréhension du COC, du Comité R¹⁵ et du Conseil d'Etat¹⁶. L'Autorité présume qu'il s'agit de la concrétisation de la « *piste à suivre* » annoncée dans le Rapport au Roi accompagnant le projet d'AR du 20 décembre 2019¹⁷. Quoiqu'il en soit, ceci (de même que

¹² Art. 6, §2 du projet de loi

¹³ Art. 9 du projet de loi ; Pour un exemple de mise en œuvre de techniques, telles que l'*intersection d'ensembles privés*, permettant à une organisation A de vérifier quelles personnes de sa liste se trouvent dans une banque de données d'une organisation B, voy. Roel Peeters, Andreas Pashalidis : Privacy-Friendly Checking of Remote Token Blacklists. IDMAN 2013, Policies and Research in Identity Management - Third IFIP WG 11.6 Working Conference, IDMAN 2013, London, UK, April 8-9, 2013. Proceedings pp. 18-33. <https://www.esat.kuleuven.be/cosic/publications/article-2303.pdf>

¹⁴ La sous-section 7bis de la LFP sous laquelle figurent les dispositions relatives à la BDC est intitulée « *Des banques de données communes* » et les AR font référence d'une part à « *la banque de données commune Terrorist Fighters* » (ci-après « BDC FTF ») (AR du 21 juillet 2016) et, d'autre part à « *la banque de données commune Propagandistes de haine* » (ci-après « BDC PH ») (AR du 23 avril 2018) ; Voy. également le Rapport au Roi du projet d'AR BDC PH disposait que « *même si les **finalités spécifiques de la banque de données Propagandistes de haine**, ainsi que les données et informations y enregistrées, diffèrent de celles de la banque de données Terrorist Fighters*, la banque de données Propagandistes de haine poursuit le même grand objectif qui est de lutter contre le terrorisme [...] ».

¹⁵ L'exposé des motifs du projet de loi précise : « *contrairement à ce qu'indique l'Organe de contrôle de l'information policière (C.O.C.) et le Comité permanent R dans leur rapport 2020, la banque de donnée commune 'Propagandiste de haine' ne constitue pas une banque de donnée commune distincte de la banque de donnée commune 'Terrorist fighters'* » ; Ce besoin de clarification pose d'autant plus question qu'en vertu de l' [Art. 44/11/3bis](#), §3 LFP, les responsables du traitement doivent déclarer la création d'une BDC au COC et au Comité R

¹⁶ A l'occasion de l'avis n°62.629/2 - 62.630/2, rendu le 31 janvier 2018 sur deux projets d'AR, l'un modifiant l'AR BDC FTF et l'autre relatif à la BDC PH, la section de législation du Conseil d'Etat indiquait qu'« *il y a lieu d'examiner le choix de l'auteur du texte de multiplier les banques de données liées à la lutte contre le terrorisme et l'extrémisme pouvant mener au terrorisme puisqu'à côté de la banque de données commune Terrorist Fighters « T.F. » (projet n° 62.629/2) est envisagée la création d'une nouvelle banque de données commune qui concerne les « Propagandistes de haine » (projet n° 62.630/2)* » (<http://www.raadvst-consetat.be/dbx/avis/62629.pdf>, p. 15)

¹⁷ « (...) Force est de constater que le Conseil d'Etat a raison lorsqu'il évoque d'une part le manque de justification quant à la nécessité d'avoir deux arrêtés royaux distincts pour les Terrorist Fighters et les Propagandistes de haine et d'autre part la difficulté de savoir si les données concernant les E.P.V. et les personnes condamnées pour terrorisme doivent être traitées dans l'arrêté royal relatif au terrorist fighters ou aux propagandistes de haine. Fondamentalement, il s'agit d'une seule banque de données, articulée autour des différentes catégories de personnes qui peuvent y être traitées. Cependant, vu d'une l'urgence de pouvoir disposer d'une assise légale pour traiter les données concernant les E.P.V. et les personnes condamnées pour terrorisme et d'autre part la période d'affaires courantes, les auteurs ont décidé de joindre ces deux nouvelles catégories dans l'arrêté royal relatif au Terrorist Fighters, qui reprend le plus grand nombre de catégories de personnes traitées dans le cadre des banques de données communes. A terme, une fusion de l'Arrêté royal Terrorist fighters et de l'Arrêté royal propagandistes de haine est donc la piste à suivre » (Rapport au Roi Arrêté royal du 20 décembre 2019 modifiant l'Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters et l'arrêté royal du 23 avril 2018 relatif à la banque de données commune Propagandistes de haine, https://etaamb.openjustice.be/fr/arrete-royal-du-20-decembre-2019_n2019031161.html).

l'énumération dans la loi de tous les services ayant accès à la BDC¹⁸) ne constitue pas pour autant une modification anodine puisque, par exemple, le service des cultes et de la laïcité, qui n'avait jusqu'à présent légalement accès qu'à la seule BDC PH¹⁹ (en vertu de l'AR du 23 avril 2018)²⁰, disposera désormais d'une base légale pour accéder à « *toute* » la BDC.

11. Par ailleurs, à la lecture de ces modifications et du nombre de services, « *centralisés* » dans le projet, ayant accès à la BDC, un doute subsiste quant au sort que le demandeur entend réserver à l'ensemble des « **47 services partenaires** » ayant accès à la BDC dont il est question dans le Rapport d'activité 2019 du Comité R²¹. L'Autorité estime qu'il convient de clarifier ce point.
12. L'Autorité souligne enfin que son prédécesseur en droit – la Commission de la protection de la vie privée – ont rendu de nombreux avis sur des projets de normes législatives et réglementaires relatives à la BDC²². Bien que la compétence de l'Autorité soit aujourd'hui²³ limitée par la compétence du COC et du Comité R, l'Autorité y renvoie pour les aspects qui ne sont pas couverts par le présent avis.

b) Concernant les Task Forces Locales

13. Il est par ailleurs prévu que les données à caractère personnel des personnes concernées (couvertes par la notion d'« *entité* », susmentionnée) devront être consultées par les services de base et les services partenaires en vue de la (1) la concertation coordonnée entre les services de base et les services partenaires, (2) la nécessité stratégique, tactique ou opérationnelle de traiter en commun des données à caractère personnel et des informations pour exercer les missions respectives des services de base et des services partenaires, (3) l'aide à la prise de décisions par les autorités administratives

¹⁸ A propos de laquelle l'exposé des motifs précise qu'elle est réalisée « *dans un souci de centralisation et de lisibilité* »

¹⁹ Et non aux données que la BDC (F)TF était censée contenir

²⁰ Un rapport des Comités R et P, sur les services d'appui de l'OCAM, indique à ce propos : « *Au cours de l'audition du 10 juillet 2020, le service des cultes et de la laïcité nous a indiqué avoir un accès complet à la BDC, et donc avoir la possibilité de l'alimenter. Cependant il s'est avéré qu'il n'y a aucune base légale leur permettant cet accès complet (ils n'ont accès légalement qu'à la BDC PH par interrogation directe). Cet accès complet est pourtant nécessaire selon eux, afin qu'ils puissent consulter directement la BDC dans le cadre de leurs compétences. Ils avancent essentiellement deux arguments pour expliquer ce choix d'un accès complet :*

-le service des cultes et de la laïcité doit avoir la possibilité d'alimenter la BDC si cela s'avère pertinent (p. ex. les personnes morales non encore intégrées dans la BDC mais qui pourraient l'être)

-les recherches effectuées mensuellement ne sont pas possibles avec un système de « HIT, NO HIT ».

Début novembre 2020, le service laïcité et cultes a précisé qu'ils travaillaient actuellement avec l'OCAM afin de régulariser leur accès complet à la BDC. En attendant, il a été décidé de réduire leur accès à la BDC à un HIT – NO HIT. Ils ont donc toujours accès à l'entièreté des entités de la BDC à ce stade car la police fédérale, gestionnaire technique de la BDC, ne peut diviser ces accès sur le plan technique » (Enquête de contrôle sur les services d'appui de l'OCAM l'AR du 17 août 2018, note 51, p. 24

(<https://www.comiteri.be/images/pdf/enquetes/2%20F%20TO%202020%20278%20Nouveaux%20services%20dappui%20OCAM.pdf>)

²¹ Voy. https://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2019.pdf, p. 89

²² Avis n°57/2015 du 16 décembre 2015, n°31/2016 du 29 juin 2016, 4/2018 du 17 janvier 2018 et 5/2018 du 17 janvier 2018 également.

²³ Depuis l'entrée en vigueur de la loi du 22 mai 2019 modifiant diverses dispositions relatives à la gestion de l'information policière (MB 19.06.2019)

ou à la prise de décisions de police administrative ou judiciaire et (4) l'analyse, l'évaluation de la menace et le suivi, en ce compris la prise de mesures, des entités enregistrées dans BDC et l'analyse, l'évaluation et le suivi du phénomène du terrorisme et de l'extrémisme lorsqu'il peut mener au terrorisme sur base d'une évaluation de la menace.

14. C'est dans cette optique que l'exposé des motifs précise que « *l'objectif est aussi, dans le cadre de la stratégie T.E.R.²⁴, de mettre l'accent sur la nécessaire concertation entre professionnels de la sécurité à propos des données contenues dans la banque de données commune T.E.R. lesquels doivent notamment s'entendre sur l'opportunité de la prise de mesures lorsqu'une entité est enregistrée dans la banque de données commune* ». Le projet de loi entend rencontrer cet objectif à travers les dispositions du chapitre 3 consacré à la concertation au sein des Task Forces Locales (ci-après « TFL »).

II. Examen

II.1. Principes de prévisibilité et de légalité

15. Conformément à l'article 6.3 du RGPD, lu à la lumière du considérant 41²⁵ du RGPD, le traitement de données à caractère personnel jugé nécessaire au respect d'une obligation légale²⁶ et/ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement²⁷ doit être régi par une réglementation qui soit claire et précise et dont l'application doit être prévisible pour les personnes concernées. En outre, selon l'article 22 de la *Constitution*, il est nécessaire que les "éléments essentiels" du traitement de données soient définis au moyen d'une norme légale formelle.

Ingérence

16. En ce qui concerne le degré d'ingérence, l'Autorité relève que le projet présente une **ingérence importante dans les droits et libertés des personnes concernées** et ce, pour les raisons suivantes :

²⁴ Cette stratégie, annoncée par l'OCAM le 8 septembre 2021, est l'actualisation du Plan d'Action Radicalisme (Plan R – publié en 2005 et actualisé une première fois en 2015) et sa transformation en une note stratégique Extrémisme et Terrorisme (<https://ocam.belgium.be/wp-content/uploads/2021/09/Note-strategique-Extrémisme-et-Terrorisme.pdf>)

²⁵ "41. Lorsque le présent règlement fait référence à une base juridique ou à une mesure législative, cela ne signifie pas nécessairement que l'adoption d'un acte législatif par un parlement est exigée, sans préjudice des obligations prévues en vertu de l'ordre constitutionnel de l'État membre concerné. Cependant, cette base juridique ou cette mesure législative devrait être claire et précise et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice de l'Union européenne (ci-après dénommée « Cour de justice ») et de la Cour européenne des droits de l'homme".

²⁶ Art. 6.1.c) du RGPD.

²⁷ Art. 6.1.e) du RGPD.

- le traitement porte sur des « *données sensibles* » au sens des articles 9 et 10 du RGPD ;
- le traitement de données à caractère personnel a lieu à des fins de contrôle et/ou de surveillance ;
- le traitement de données à caractère personnel implique le croisement ou la combinaison de différentes informations concernant la personne concernée issues de deux (ou plusieurs) opérations de traitement de données effectuées à l'origine pour des finalités différentes et/ou par différents responsables du traitement, d'une manière telle qui outrepassa les attentes raisonnables de la personne concernée ;
- le traitement de données à caractère personnel est susceptible de concerner des personnes vulnérables²⁸ (notamment des mineurs, des réfugiés, demandeurs d'asile ou migrants, des personnes présentant des troubles mentaux, ...) ; et
- le traitement de données à caractère personnel complique l'exercice d'un droit par les personnes concernées.

17. L'Autorité souligne en outre que la participation de nouveaux acteurs a pour effet (et même pour objet) d'augmenter la quantité de données à caractère personnel traitées et de permettre la combinaison de ces données, engendrant par voie de conséquence une aggravation de l'ingérence dans les droits et libertés des personnes concernées.

18. Par conséquent, en vertu de l'article 22 de la *Constitution*, il est nécessaire que les "éléments essentiels" des traitements **relatifs aux données enregistrées dans la BDC ET aux données communiquées à l'occasion des concertations en TFL** soient définis dans une norme de rang législatif. Ces éléments sont : la (les) finalité(s) précise(s) et concrète(s)²⁹ à la lecture de laquelle (desquelles) on peut déjà apercevoir les traitements de données qui seront mis en place pour sa (leur) réalisation, l'identité du (des) responsable(s) du traitement, les (catégories de) données qui sont nécessaires à la réalisation de cette (ces) finalité(s), le délai de conservation des données³⁰, les (catégories de) personnes concernées dont les données seront traitées, les (catégories de)

²⁸ Il est question de personnes vulnérables lorsqu'il existe un « (...) *déséquilibre des pouvoirs accru qui existe entre les personnes concernées et le responsable du traitement, ce qui signifie que les premières peuvent se trouver dans l'incapacité de consentir, ou de s'opposer aisément au traitement de leurs données ou d'exercer leurs droits* » (S. Wattier et M. Nihoul, « Chapitre 1 - La protection de la personne en situation de vulnérabilité par le droit des libertés publiques dans l'environnement numérique » in H. Jacquemin et M. Nihoul (dir.), *Vulnérabilités et droits dans l'environnement numérique*, Bruxelles, Larcier, 2018, pp. 14 et sv.).

²⁹ Voir aussi l'article 6.3 du RGPD.

³⁰ La Cour constitutionnelle a déjà reconnu que "le législateur pouvait régler de manière générale les conditions de conservation des données à caractère personnel, ainsi que la durée de cette conservation" ; Arrêt n° 29/2018 du 15 mars 2018, point B. 23.

destinataires auxquels les données seront communiquées³¹, les circonstances dans lesquelles elles seront communiquées ainsi que l'éventuelle limitation des obligations et/ou des droits visé(e)s aux articles 5, 12 à 22 et 34 du RGPD.

Délégation au Roi

19. L'article 22 de la Constitution interdit au législateur de renoncer à la possibilité de définir lui-même quelles sont les intrusions qui peuvent restreindre le droit au respect de la vie privée³². Dans ce contexte, une délégation au Roi « *n'est pas contraire au principe de légalité, pour autant que cette délégation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur* »³³.
20. En l'espèce, le projet de loi habilite notamment le Roi à déterminer les catégories d'entités (c'est-à-dire notamment les catégories de personnes concernées) à propos desquelles les données sont traitées (art. 6), les finalités de l'interconnexion (c'est-à-dire les finalités d'un traitement de données à caractère personnel) et les catégories de données à caractère personnel interconnectées (art. 9, §1^{er}, al. 2), d'autres missions (c'est-à-dire potentiellement d'autres finalités de traitement) de la TFL (art. 33, §2, *in fine*) et les modalités d'exercice des droits de rectification, d'effacement ou d'accès (indirect) (art. 40).
21. S'agissant d'éléments essentiels du traitement, l'Autorité estime que les dispositions du projet d'arrêté (et les éléments correspondant du Rapport au Roi) doivent figurer dans le projet de loi (et dans le commentaire des articles concernés) et que, par conséquent, les délégations contenues aux articles 6, 9, 33 et 40 du projet de loi doivent être expressément limitées au modalités d'exécution des éléments essentiels qui doivent quant à eux être déterminés par la loi.

³¹ Voir par exemple, Cour constitutionnelle, arrêt n° 29/2018 du 15 mars 2018, point B.18, et Cour constitutionnelle, Arrêt n° 44/2015 du 23 avril 2015, points B.36.1 e.s.

³² Avis n° 63.202/2 donné 26 avril 2018 du Conseil d'Etat sur un avant-projet de loi "instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, Doc. parl. Chambre, 54-3185/001, p 121-122.

Voir dans le même sens les avis suivants du Conseil d'Etat :

- Avis n° 26.198/2 donné le 2 février 1998 sur un avant-projet devenu la loi du 11 décembre 1998 "transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données", Doc. parl., Chambre, 1997-1998, n° 49-1566/1, p. 201.
- Avis n° 33.487/1/3 des 18 et 20 juin 2002 sur un avant-projet devenu la loi du 22 août 2002 "portant des mesures en matière de soins de santé", Doc. parl., Chambre, 2002-2003, n° 2125/2, p. 539.
- Avis n° 37.765/1/2/3/4 donné le 4 novembre 2004 sur un avant-projet devenu la loi-programme du 27 décembre 2004, Doc. parl., Chambre, 2004-2005, n° 1437/2.

³³ Voir aussi Cour Constitutionnelle : arrêt n° 29/2010 du 18 mars 2010, point B.16.1 ; arrêt n° 39/2013 du 14 mars 2013, point B.8.1 ; arrêt n° 44/2015 du 23 avril 2015, point B.36.2 ; arrêt n° 107/2015 du 16 juillet 2015, point B.7 ; arrêt n° 108/2017 du 5 octobre 2017, point B.6.4 ; arrêt n° 29/2018 du 15 mars 2018, point B.13.1 ; arrêt n° 86/2018 du 5 juillet 2018, point B.7.2 ; avis du Conseil d'Etat n° 63.202/2 du 26 avril 2018, point 2.2.

Remarque particulière relative à la journalisation

22. L'art. 8 du projet de loi porte sur la journalisation des traitements relatifs aux données figurant dans la BDC. Le commentaire de cet article précise que cette disposition est une version modifiée de l'art. 44/4, §2, al. 2 LFP, en ce que l'énumération des traitements qui doivent faire l'objet d'une journalisation est exhaustive. L'Autorité est favorable à une telle énumération exhaustive, mais constate que l'art. 8, §1^{er} du projet de loi habilite le Roi à déterminer « *d'autres types* » de traitements pour lesquels les fichiers de journalisation sont établis. A cet égard, compte tenu de la volonté d'exhaustivité manifestée par le demandeur, l'Autorité estime qu'il convient d'omettre cette habilitation et de prévoir que « *l'ensemble des traitements des données figurant dans la banque de données communes, en ce compris leur enregistrement, font l'objet d'une journalisation* ».
23. L'Autorité constate que l'énumération figurant à l'art. 8, §1^{er} est muette quant à la journalisation de « *l'extraction* » des listes (visée à l'art. 26, §1^{er}) par les services ayant un droit de lecture, pour un « *traitement interne* ». Cette disposition prévoit en outre que cette extraction - que l'Autorité comprend comme la possibilité de copier les données de cette liste - doit être effectuée par un membre du personnel titulaire d'une habilitation de sécurité « *secret* ». L'Autorité précise que le contrôle du respect de cette condition implique de lier la possibilité d'une extraction par ces services à l'existence d'une obligation légale de journalisation de cette extraction (opposable à ces services³⁴).
24. Le commentaire de l'art. 8 précise par ailleurs que « *la collecte* » est remplacé par « *l'enregistrement* » pour s'adapter à la « *réalité IT* ». L'Autorité comprend que cet argument signifie en réalité que la BDC ne collecte pas (et non pas que c'est un système informatique et son fonctionnement qui détermine la manière dont un texte de loi doit être libellé³⁵). En ce sens, sous l'importante réserve qu'il y a lieu de se placer du point de vue du responsable du traitement et non de la banque de données³⁶, l'Autorité estime que cet argument est admissible. Toutefois, l'effectivité du principe d'exactitude des données repose en grande partie sur la possibilité de vérifier le respect de la réglementation relative à la protection des données dès la collecte de ces données (et sur le lieu de celle-ci). L'Autorité estime donc qu'il y a lieu de prévoir que la collecte des données susceptibles d'être enregistrées dans la BDC doit avoir été journalisée. Les normes organiques des services disposant d'un droit d'écriture devront donc être modifiées en ce sens.
25. L'Autorité estime par ailleurs que ce même souci d'effectivité implique de prévoir les modalités (en ce compris la périodicité) du contrôle des fichiers de journalisation dans le projet et dans les normes

³⁴ Sur cette question voy. *infra*

³⁵ Ce qui ne serait bien entendu pas admissible

³⁶ Sur cette question voy. *infra*

organiques des services partenaires pour les traitements « *locaux* » (mais le pouvoir Exécutif peut valablement être habilité à le faire).

26. **Dans la perspective d'une modification des normes organiques des services partenaires**, comme il sera davantage explicité lors de l'analyse des dispositions relatives aux responsables du traitement, il convient de noter que le respect du principe de légalité implique également d'être attentif à l'adéquation des finalités des traitements prévus, par rapport à la **compétence du législateur**³⁷. L'Autorité attire l'attention du demandeur sur le fait qu'en cas de nouvelle réforme de l'Etat, la licéité du traitement des données enregistrées dans la BDC (et/ou leur communication) est susceptible d'être affectée jusqu'à l'adoption d'un accord de coopération.

II.2. Finalités

27. En vertu de l'article 5.1.b) du RGPD, 28, 2° et 75, 2° LTD, un traitement de données à caractère personnel n'est autorisé que pour des finalités déterminées, explicites et légitimes. Par ailleurs, en vertu de l'article 6.3. du RGPD, lu à la lumière du considérant 41 du RGPD et de l'article 22 de la Constitution, la finalité doit être formulée de manière suffisamment explicite et précise pour que les personnes concernées connaissent clairement les raisons exactes qui ont conduit au traitement de leurs données à caractère personnel. À la lecture de cette finalité, celles-ci doivent pouvoir déduire quels traitements de données sont nécessaires pour l'atteindre.
28. L'art. 3 du projet de loi contient la **finalité générale** des traitements de données prévus par le projet, à savoir « *la lutte, la prévention et le suivi du terrorisme et de l'extrémisme, lorsqu'il peut mener au terrorisme* ». Cette disposition précise également que cette finalité est poursuivie par les services de base ET les services partenaires, « *chacun dans le cadre de ses compétences légales* ».
29. L'art. 5 du projet de loi énonce les **4 finalités spécifiques** « *de la BDC* ». Il s'agit de la (1) la concertation coordonnée entre les services de base et les services partenaires, (2) la nécessité stratégique, tactique ou opérationnelle de traiter en commun des données à caractère personnel et des informations pour exercer les missions respectives des services de base et des services partenaires, (3) l'aide à la prise de décisions par les autorités administratives ou à la prise de décisions de police administrative ou judiciaire et (4) l'analyse, l'évaluation de la menace et le suivi, en ce compris la prise de mesures, des entités enregistrées dans BDC et l'analyse, l'évaluation et le suivi du phénomène du

³⁷ Sur la question de (l'absence de) compétence de l'autorité fédérale pour imposer des obligations à toutes les autorités ayant accès aux banques de données communes, y compris celles relevant des entités fédérées, voy. l'avis de la Section de législation du conseil d'Etat n°59.515/2 du 6 juillet 2016 rendu sur un projet d'arrêté royal „relatif à la banque de données commune foreign terrorist fighters et portant exécution de certaines dispositions de la section Irebis « de la gestion des informations » du chapitre IV de la loi sur la fonction de police”, points 2.2. à 2.3.3. (<http://www.raadvst-consetat.be/dbx/avis/59515.pdf>)

terrorisme et de l'extrémisme lorsqu'il peut mener au terrorisme sur base d'une évaluation de la menace.

30. Tout d'abord, l'Autorité répète la demande formulée dès 2015 par la CPVP, à savoir que les nécessités stratégiques, tactiques et opérationnelles soient distinguées les unes des autres et décrites précisément dans la loi ou un arrêté d'exécution³⁸.
31. En outre, l'Autorité rappelle qu'elle est favorable à la détermination des finalités d'une banque de données (ou d'un registre), mais qu'il n'en demeure pas moins que le respect de l'article 5.1.b) du RGPD (de même que des art. 28, 2° et 75 LTD) impose la **détermination des finalités des traitements** de données à caractère personnel (dont l'enregistrement dans une banque de données spécifique constitue un exemple parmi d'autres). Par conséquent, il y a lieu de distinguer les finalités liées à la création d'une banque de données, des finalités des différents traitements réalisés par chacun des services relativement à ces données (collecte, concertation en TFL, enregistrement dans la BDC, communication à d'autres services, transferts internationaux, etc...).
32. En ce qui concerne la collecte, il sera simplement renvoyé (dans le commentaire) aux législations organiques des services de base et des services partenaires. En revanche, il devra être démontré (dans le commentaire de l'art. 6), pour chacun des services disposant d'un droit d'écriture, en quoi la finalité de chacun des traitements ultérieurs de ces données est compatible avec la finalité pour laquelle elles ont été collectées.
33. En ce qui concerne les traitements ultérieurs réalisés par les services partenaires, l'art. 6, §2, 2° du projet de loi permet le traitement des données opérationnelles policières, contenues dans la BDC, « *qui sont adéquates, pertinentes et non excessives au regard des missions* [de prévention et de suivi du terrorisme et de l'extrémisme, lorsqu'il peut mener au terrorisme (...)] de ces services, chacun dans le cadre de ses compétences légales] *et des finalités* [de la BDC] », par les services de base et les services partenaires disposant d'un droit de lecture³⁹.
34. L'Autorité précise que la détermination des catégories de données à caractère personnel relatives aux entités contenues dans la BDC qui sont accessibles de manière licite, c'est-à-dire communicables aux services partenaires (ou même la simple interrogation de la BDC) dépend à la fois de l'existence d'une base légale pour la communication ET des finalités propres de ces services partenaires. En d'autres termes, quelles que soient les limitations techniques du support d'enregistrement⁴⁰, **l'enregistrement**

³⁸ Avis 57/2015, *op. cit.*, point 54

³⁹ A noter qu'en vertu du projet d'AR, seuls la DG Sécurité et Prévention, la DG Affaires Consulaires et le Service des cultes et de la laïcité sont limités à une interrogation (sous forme de hit – no hit) de la BDC, alors que tous les autres disposent d'un droit de lecture.

⁴⁰ Voy. l'exemple mentionné *supra* concernant le service des cultes

dans la BDC ne peut aboutir à ce qu'un service traite (ne fut-ce qu'en consultant) des données à caractère personnel qu'il ne serait pas autorisé à traiter en vertu de ses finalités propres.

35. Par conséquent, soit (1) les finalités de traitements auxquelles leurs lois organiques les soumet leur permettent déjà d'avoir accès à ces données (dans ce cas, il convient de faire référence aux normes applicables et de préciser dans le commentaire de l'art. 6 que la disposition en projet se limite à prévoir une modalité technique de communication), soit (2) le projet entend prévoir une nouvelle finalité d'accès pour ces services (dans ce cas, il convient de le prévoir expressément, d'en justifier le caractère nécessaire et proportionné ET de prévoir une modification des lois organiques concernées en ce sens), soit enfin (3) le demandeur considère que la communication actuelle, par exemple sous forme de simple avis (favorable ou négatif), de rapport de police ou de demande de prise de mesures est trop limitée et entend l'étendre (et dans ce cas, outre l'adaptation des lois organiques respectives, il convient de dûment démontrer le caractère nécessaire et proportionné de l'augmentation de la quantité de données communiquées).
36. Le cas échéant et, pour autant que le caractère nécessaire et proportionné d'une telle communication et/ou de tels accès soient démontrés, le projet devra prévoir une adaptation (valable pour le futur) des normes organiques des services dont la finalité n'est actuellement pas libellée d'une manière à permettre un traitement ultérieur compatible.
37. L'Autorité précise que les finalités de ces accès par les services partenaires doivent être déterminées **pour chaque catégorie de donnée**. Il ne peut en effet être question, comme le libellé actuel de l'art. 6, §2, 2° du projet de loi permet de le craindre, de communiquer le tout⁴¹ et de laisser aux autorités destinataires la responsabilité de sélectionner ce qu'elles ont le droit de consulter. A titre d'exemple, le libellé du projet doit permettre de comprendre que des catégories particulières de données ne peuvent en aucun cas être communiquées (ou rendues accessibles) à l'Administration générale de la Trésorerie ou que la présence d'une entité.
38. L'Autorité précise à toutes fins utiles que **ne peuvent être considérées comme légitimes**, des finalités liées à la **facilité** pour les services de base (qui, par exemple, en échange de la communication de données excédant de très loin celles que les services partenaires sont habilités à traiter pour les

⁴¹ Le rapport du Comité R confirme cette impression en mentionnant que « *pour les services de renseignement, l'intérêt des BDC est de pouvoir retrouver en un seul endroit toutes les informations dont disposent leurs partenaires et diffuser, par un canal unique, les informations non classifiées dont ils disposent* » (Comité R, Enquête de contrôle sur le suivi par les services de renseignement et de sécurité belges des détenus condamnés pour terrorisme et/ou identifiés comme radicalisés pendant et après leur détention, 31 mai 2022, p.18 (https://www.comiteri.be/images/pdf/enquetes/TERRO_PRISON_UNCLASS_FR.pdf)); Sur l'opportunité d'avoir recours à l'*intersection d'ensembles privés*, voy. la note de bas de page n°13 (*supra*)

besoins de leurs missions, ne devraient plus communiquer des listes⁴² ou recevraient automatiquement les données relatives aux entités, sans avoir à les collecter auprès des services partenaires)⁴³, ni à un **impact budgétaire**⁴⁴.

39. L'Autorité rappelle au passage que la fixation de limites ou l'énonciation, dans l'exposé des motifs, de circonstances dans lesquelles un traitement serait constitutif d'un détournement de finalité constitue une bonne pratique, en particulier lorsque – comme c'est le cas en l'espèce – l'ingérence est particulièrement importante ou que les risques de détournement de finalité sont élevés.
40. En ce qui concerne l'**interconnexion** visée à l'art. 9 du projet de loi, l'Autorité estime qu'il convient de prévoir que l'interconnexion de la BDC avec des sources authentiques en peut en aucun cas permettre à des autorités ne disposant pas d'un accès légal à ces sources, de se voir accéder aux données contenues dans ces sources authentiques. Cette précaution, requise par le choix de la centralisation plutôt que par la mise en place d'un système de type banque-carrefour⁴⁵, s'inscrit également dans l'optique selon laquelle la fixation de limites ou l'énonciation, dans l'exposé des motifs, de circonstances dans lesquelles un traitement serait constitutif d'un détournement de finalité constitue une bonne pratique.

Observations relatives aux TFL

41. Les art. 31 et sv. du projet de loi prévoient (ou modifient) les traitements de données effectués lors des concertations en TFL. Même si ces dispositions appellent certaines observations, l'Autorité tient à préciser qu'elle **accueille très positivement l'encadrement législatif des traitements de données effectués lors des concertations en TFL**.
42. En ce qui concerne les finalités des traitements, l'art. 31 du projet de loi dispose que les traitements de données à caractère personnel pertinentes, sont échangées au sein d'une ou plusieurs plateformes de concertation créées auprès de chaque arrondissement judiciaire, appelée TFL, « en vue d'assurer

⁴² Voy. le rapport des Comités R et P, sur les services d'appui de l'OCAM indiquant que « *précédemment, chaque mois, l'OCAM envoyait une liste de personnes établies comme prédicateur de haine au Service des Cultes et de la Laïcité (DGWL). Le Service comparait cette liste avec les états de traitements des ministres du culte et des délégués du Conseil Central Laïque. A présent, le Service a accès à la Banque de données commune* » (*op. cit.*, p. 24)

⁴³ Voy. le rapport du Comité R indiquant que « *pour les services de renseignement, l'intérêt des BDC est de pouvoir retrouver en un seul endroit toutes les informations dont disposent leurs partenaires (...)* » (Comité R, Enquête de contrôle sur le suivi par les services de renseignement et de sécurité belges des détenus condamnés pour terrorisme..., *op. cit.*, p. 18)

⁴⁴ La Cour de justice estime en effet « *que le manque de ressources allouées aux autorités publiques ne saurait en aucun cas constituer un motif légitime permettant de justifier une atteinte aux droits fondamentaux garantis par la Charte* » (CJUE, 1^{er} août 2022, C-184/20, OT c. Vyriausioji tarnybinės etikos komisija, §89)

⁴⁵ Dont l'Autorité ne prétend pas qu'il ne serait pas critiquable

l'enrichissement des données à caractère personnel et informations relatives aux entités ainsi que le suivi et la prise de mesures à l'égard des entités validées dans la [BDC] ».

43. Alors que l'art. 31 du projet de loi semble⁴⁶ mettre l'accent sur la finalité d'enrichissement de la BDC, à la lecture du commentaire, l'Autorité comprend que cette disposition entend davantage, dans un contexte *post* affaire Conings⁴⁷, prévoir une obligation d'échange « *loyal* » de données (classifiées ou non), concernant « *ce phénomène particulièrement sérieux* », en provenance de services tenus d'alimenter la BDC ou non. Le caractère accessoire de l'enrichissement de la BDC semble confirmé par le passage du commentaire en vertu duquel « *ces informations sont classifiées ou confidentielles, elles ne pourront être mentionnées dans le rapportage des task force locales* »⁴⁸.
44. Le libellé actuel de l'art. 31 revient à justifier un traitement de données (l'échange) par un autre traitement de données (l'enregistrement). Il convient donc de reformuler cette disposition en veillant à l'aligner sur son commentaire (par exemple abandonnant la logique « *des banques de données* », c'est-à-dire en considérant l'enregistrement dans la BDC comme l'un des traitements susceptibles d'être réalisés pour les finalités de la concertation en TFL).
45. Le commentaire introductif du chapitre 3 précise que « *le résultat de cette concertation est transmis à l'autorité compétente pour décider de la mesure en question* » et le commentaire de l'art. 31 ajoute que « *services sont tenus de n'échanger que les données à caractère personnel et les informations qu'ils ont le droit de traiter dans le cadre de leurs missions* »⁴⁹.
46. Les finalités de la communication de données aux services invités à participer aux TFL, en vertu de l'art. 32 du projet de loi, doivent être libellées de manière à ce qu'à la lecture de celles-ci, il soit possible aux personnes concernés, mais aussi aux participants, de savoir si l'invitation des « *services invités* » se limite à leur demander de communiquer les données en leur possession et/ou à prendre certaines mesures ou si (et, le cas échéant, dans quelles circonstances) les finalités des traitements de données effectués dans le cadre des TFL, en combinaison avec les missions et le « *need to know* » des services invités justifie que certaines catégories de données (devant à tout le moins être déterminables) soient communiquées aux services invités.
47. Il conviendra également de déterminer clairement si les TFL sont des **plateformes de concertation organisées en application de l'art. 458ter CP**. En effet, si tel est le cas, l'ensemble du chapitre 3 devra être revu en vue d'y déterminer la finalité de manière précise (et d'y démontrer *in concreto* le

⁴⁶ Sans doute en raison du fait qu'il ouvre le Chapitre 3 intitulé « *Enrichissement des données relatives aux entités et suivi d'une entité validée dans la banque de données commune T.E.R.* »

⁴⁷ Sur cette question, voy. l'analyse de proportionnalité, *infra*

⁴⁸ En d'autres termes, elles ne pourront pas être enregistrées dans la BDC préalablement à leur déclassification

⁴⁹ La version néerlandaise dispose « *zijn ertoe gehouden enkel de persoonsgegevens en de informatie uit te wisselen waarvoor zij het recht hebben ze te verwerken in het kader van hun opdracht* »

caractère nécessaire et proportionné des traitements envisagés)⁵⁰. **Le cas échéant, compte tenu de l'importance des adaptations requises, l'Autorité souhaite que le projet adapté lui soit à nouveau soumis pour avis avant son adoption.**

Finalité du droit de communiquer certaines catégories de données à caractère personnel couvertes par le secret professionnel⁵¹

48. L'art. 19, al. 3 du projet dispose que « *l'article 458 du Code pénal ne peut être invoqué lorsque les services de base ou les services partenaires exercent leur droit d'écriture dans la banque de données commune T.E.R. conformément à la présente section* ». Le commentaire de cet article précise que « *les services de base ou les services partenaires qui alimentent la banque de données commune T.E.R. par le biais de leur droit d'écriture ne peuvent se voir opposer l'article 458 du Code pénal relatif à la violation du secret professionnel dans ce contexte* ». L'Autorité déduit du commentaire que cette disposition ne vise pas à empêcher les services d'invoquer le secret professionnel pour s'opposer à l'alimentation de la BDC, mais à permettre que l'alimentation ne puisse jamais être considérée comme une violation du secret professionnel.
49. Si cette interprétation est exacte, cela revient à créer une nouvelle exception légale au secret professionnel et il serait souhaitable que le projet modifie le Code pénal en vue d'y introduire cette nouvelle typologie d'exception. Le cas échéant, il conviendrait cependant de **renoncer à la logique des banques de données**. En effet, en soumettant l'exception au seul « *exercice du droit d'écriture* » par les services de base ou les services partenaires⁵² et en s'abstenant de déterminer des conditions précises à l'application de cette exception, le projet risque d'avoir pour effet que même les informations dont la communication serait totalement inutile pour les finalités mentionnées à l'art. 3 du projet de loi, ne soient plus révélées aux intervenants soumis au secret professionnel par crainte de leur révélation. Par ailleurs, une définition claire de la finalité du droit de communiquer certaines catégories de données à caractère personnel couvertes par le secret professionnel, est une mesure protectrice de la personne concernée, mais également du professionnel participant⁵³. Il convient donc de veiller, lors de la reformulation du commentaire de l'art. 19, à ce que, à la lecture de la disposition, une

⁵⁰ Voy. à ce sujet, les observations formulées par l'Autorité à l'occasion de son avis n°254/2022 du 1^{er} décembre 2022 (<https://www.autoriteprotectiondonnees.be/publications/avis-n-254-2022.pdf>); Concernant l'analyse de la proportionnalité, voy. *infra*

⁵¹ L'Autorité rappelle qu'indépendamment du secret professionnel, l'alimentation de la BDC doit reposer sur une obligation légale émanant d'un **législateur compétent** pour édicter une obligation opposable aux autorités concernées.

⁵² Ce qui, pour prendre une analogie, revient à considérer qu'un véhicule d'urgence ne peut jamais être considéré comme commettant une infraction au Code de la route

⁵³ A la lecture de cette finalité, le praticien devrait être à même de répondre aux questions du type de celles soulevées par le prof. Jacques Fierens et figurant dans les actes de la journée de réflexion du 30 janvier 2018 intitulée « *Le secret professionnel en danger – la concertation de cas en question* », pp. 21 et 22 (https://www.liguedh.be/wp-content/uploads/2018/11/Etude_LDH_DOSSIER_458TER_avril_2018.pdf); Sur cette question voy. également les nombreuses observations formulées par l'Autorité à l'occasion de son avis n°254/2022 du 1^{er} décembre 2022 (<https://www.autoriteprotectiondonnees.be/publications/avis-n-254-2022.pdf>)

interprétation susceptible d'engendrer de telles conséquences négatives pour le fonctionnement d'une institution que le secret a vocation à protéger, puisse être écartée.

50. Si l'exception au secret professionnel entend répondre à la problématique soulevée par le décès du policier Thomas Monjoie⁵⁴, il y a surtout lieu de déterminer ce que le destinataire de l'information couverte par le secret professionnel a la possibilité et/ou l'obligation de faire avec les données communiquées. En effet, si la personne est considérée comme dangereuse par les services de police, cette information ne peut servir qu'à justifier auprès du personnel médical, le fait pour les services de police de rester sur les lieux en vue de veiller à la protection du personnel médical. Si, indépendamment de la dangerosité, il s'agit de communiquer au personnel de santé des éléments sur base desquels des troubles psychologiques ont pu être suspectés (telles des déclarations en vertu desquelles l'intéressé voulait s'en prendre à des policiers), il convient de déterminer l'obligation à laquelle le personnel médical serait soumise sur base de ces informations. En effet, d'une part, la personne ayant communiqué le secret peut délier le confident nécessaire de son obligation, et d'autre part, dans cette affaire, le personnel médical ne s'est pas opposé à l'internement volontaire. Il n'a simplement pas eu le temps de prendre en charge l'intéressé, laissé sans surveillance, avant sa disparition de la salle d'attente⁵⁵. Par conséquent, la finalité du traitement de donnée envisagée par le demandeur, dans un cas de figure tel que celui-là, doit être précisée, de manière à permettre d'en démontrer le caractère nécessaire et proportionné.
51. En outre, l'Autorité constate que, dans son libellé actuel, cette disposition ne s'applique qu'aux confidentiels nécessaires d'informations couvertes par un secret auquel l'art. 458 est applicable (par opposition au secret de l'instruction⁵⁶, au devoir de réserve ou aux obligations de secret trouvant leurs sources dans les statuts ou même dans un contrat⁵⁷ dont la conclusion serait une condition établie par la loi⁵⁸ en vue de permettre la réalisation de certaines tâches ou d'accéder à certaines données).
52. Par ailleurs, au sein de la liste des services partenaires, seuls certains intervenants au sein des services de l'aide à la jeunesse, des Maisons de justice et le personnel de santé et intervenants sociaux employés par l'OE sont susceptibles d'être concernés par l'obligation de secret visée à l'art. 458 CP.

⁵⁴ Dont il est question dans l'exposé des motifs (p. 6) ; Sur cette question, voy. Com. Justice et Intérieur, 14 novembre 2022, Com. 929, pp. 2 et sv.

(<https://www.lachambre.be/doc/ccra/pdf/55/ac929.pdf>)

⁵⁵ *Ibidem*, pp. 7 et sv.

⁵⁶ Dont il est d'ailleurs spécifiquement question à l'alinéa suivant

⁵⁷ Qu'il s'agisse d'un contrat de travail ou d'un NDA

⁵⁸ En conséquence de quoi un simple raisonnement en termes de hiérarchie des normes aboutirait à vider de son sens l'obligation légale

Cependant, les concernant, l'art. 458 CP s'oppose à la communication des informations couvertes par le secret à leur direction qui, elle, n'est pas soumise au secret professionnel (et ne violerait donc aucune obligation de secret en alimentant la BDC). Par conséquent, si l'intention du demandeur et d'appliquer cette disposition à d'autres intervenants et/ou autorités, il conviendra de préciser, dans le commentaire de l'article 19, lesquelles et de quelle manière.

53. Concernant le secret professionnel des participants à une concertation en **TFL**, l'Autorité s'étonne du fait qu'alors que l'avant-dernier alinéa l'art. 32, §1^{er} du projet de loi prévoit expressément la possibilité pour d'autres services, organes ou instances, d'être invité à participer à une TFL, aucune dérogation à l'art. 458 CP se soit prévue. Le cas échéant, il sera veillé à définir clairement la **finalité du droit de communiquer** certaines catégories de données à caractère personnel couvertes par le secret professionnel. En effet, comme le rappelle le Collège des procureurs généraux (à propos des CSIL)⁵⁹, *« celui qui viole son secret professionnel parce qu'à l'occasion de la concertation, il confie des secrets qui ne concernent pas les infractions pour lesquelles la concertation a été organisée peut (...) être pénalement poursuivi. (...) Il faut par conséquent veiller à ce qu'une éventuelle communication de secrets intervienne toujours dans le cadre du but postulé et conformément aux modalités fixées de la concertation »*⁶⁰. Il en résulte que **les données des participants sont susceptibles d'être traitées à des fins répressives**. Bien entendu, les éléments constitutifs de ces traitements figurent dans le Code d'instruction criminelle. Néanmoins, l'Autorité estime que le projet devrait attirer l'attention des professionnels participants quant à la possibilité d'un traitement de leurs données pour une telle finalité.

Finalités de traitement des données archivées

54. Le commentaire de l'art. 4 précise que *« contrairement à ce qui est actuellement prévu dans la loi sur la fonction de police, la phrase « sans préjudice de la loi du 24 juin 1955 relative aux archives » a été supprimée car la référence est déjà faite à l'article 7 où elle est plus pertinente. En effet, la loi relative aux archives intervient bien au moment de l'archivage et de la suppression des données à caractère personnel et constitue même une exception au principe de suppression »*. L'art. 7, §2, al. 1 du projet de loi ne prévoit cependant pas que l'archivage interviendra *« conformément à la loi du 24 juin 1955 relatives aux archives*. La mention de cette loi n'intervient qu'à l'alinéa 2 qui prévoit qu' *« à l'issue de*

⁵⁹ Voy. *infra*

⁶⁰ COL 04/2018 du 15 mars 2018, p.14 (https://www.om-mp.be/sites/default/files/u1/col04_2018_casusoverleg_fr.pdf); la circulaire recommande par ailleurs de veiller *« à ce que l'attention de tous les participants à la concertation ait été attirée là-dessus avant d'entamer la concertation »*; En ce sens, voy. également la note de clarification de l'OCAM sur la CSIL-R, p. 6 (https://ocam.belgium.be/wp-content/uploads/2020/09/note_clarification_CSIL-R-web.pdf) ainsi que l'avis n°163 du 1^{er} octobre 2018 du Conseil communautaire de l'aide à la jeunesse, p. 6 (https://www.aidealajeunesse.cfwb.be/index.php?eID=tx_nawsecuredl&u=0&g=0&hash=b76aa4435faee9de86302b2c3552dd127cbb0a21&file=fileadmin/sites/ajss/upload/ajss_super_editor/DGAJ/Documents/CCAJ/Avis_163-CCAJ-Avant-projet_de_decret_concertation_de_cas-041018.pdf)

ce délai, ces données et informations sont supprimées, sans préjudice de la loi du 24 juin 1955 relative aux archives ».

55. Il en résulte que ces données, qui doivent être archivées « *au maximum 30 ans après le dernier traitement* » (art. 7, §1^{er}) et dont les finalités de traitement sont notamment « *le traitement des antécédents dans le cadre d'une enquête judiciaire ou de renseignement de terrorisme et d'extrémisme pouvant mener au terrorisme* » (art. 7, §2, 2^o), restent entre les mains du responsable du traitement sous une forme permettant l'identification⁶¹.
56. Alors que le mécanisme de cet archivage *sui generis* (également préconisé par la CPVP⁶²) était rendu intelligible par les explications figurant à son sujet dans les travaux parlementaires relatifs à la loi du 18 mars 2014 relative à la gestion de l'information policière⁶³, la transposition de ces dispositions dans ce nouveau projet de loi permet difficilement d'apprécier le caractère légitime du traitement des données archivées.
57. Compte tenu du fait qu'en faisant précéder la suppression des données par une longue période d'archivage (qui elle-même, fait suite à une longue durée de conservation⁶⁴), certaines données à caractère personnel archivées pourront être conservées sous une forme permettant leur identification dans les archives de la BDC après leur suppression par le responsable du traitement à l'origine de leur collecte. Il en résulte la nécessité, concernant la finalité d'archivage, de (à tout le moins) intégrer une référence aux travaux préparatoires de la loi de 2014, dans le commentaire de l'art. 7 et, concernant la finalité du traitement des données archivées, d'en démontrer le caractère légitime au regard

⁶¹ Seul le résultat de l'exploitation des archives pour la finalité d'appui à la définition et à la réalisation de la politique de sécurité en matière de terrorisme et d'extrémisme pouvant mener au terrorisme est anonymisé (art. 7, §2, al. 3, 5^o), sans même que la stratégie d'anonymisation soit précisée en commentaire

⁶² Avis 57/2015, *op. cit.*, point 63

⁶³ Loi relative à la gestion de l'information policière et modifiant la loi du 5 août 1992 sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle (MB 28.03.2014), voy. Doc. Parl. Ch., 4 novembre 2013, 53-3105/001, pp. 8 et sv. (<https://www.lachambre.be/FLWB/pdf/53/3105/53K3105001.pdf>)

⁶⁴ Sauf pour les entités en « *pré-enquête* », définies comme des entités qui n'entre pas, au moment de leur enregistrement dans la BDC, dans les critères pour être considérée comme de telles entités et qui sont archivées (et non effacées) après 6 mois

du constat « *alarmant* » du COC⁶⁵ relatif à la qualité d'une autre banque de données gérée par le gestionnaire de la BDC et de la jurisprudence pertinente⁶⁶.

58. L'Autorité constate que les art. 4, 24, 46 et surtout l'art. 28⁶⁷ du projet de loi font référence à de possibles traitements ultérieurs. L'Autorité se contente de rappeler à ce propos que les données à caractère personnel ne peuvent pas être traitées ultérieurement d'une manière incompatible avec les finalités pour lesquelles elles ont été collectées. A l'occasion de son arrêt n° 29/2018, la Cour constitutionnelle a d'ailleurs rappelé que l'exigence d'un fondement légal précis et prévisible (et donc d'une finalité claire) "*s'applique d'autant plus lorsque les données à caractère personnel sont ensuite traitées par les services publics à d'autres fins que celles pour lesquelles elles ont initialement été obtenues*"⁶⁸. En d'autres termes, **le libellé de la finalité du traitement ultérieur** (par exemple la finalité de la communication aux services étrangers) **doit également permettre de déterminer la compatibilité de cette finalité avec la finalité pour laquelle les données ont été initialement collectées**.
59. Pour des raisons qui seront détaillées *infra*⁶⁹, l'Autorité estime qu'il convient de mentionner (à l'art. 4 du projet) que des statistiques seront réalisées aux **fins de la publication d'un rapport d'évaluation** (selon une périodicité à déterminer dans le projet, mais qui ne devrait pas être inférieur à tous les 3 ans) portant sur l'efficacité des moyens de traitements mis en œuvre et des autorités impliquées par la loi en projet et son arrêté d'exécution par rapport aux finalités pour lesquelles les données ont été enregistrées dans la BDC.
60. L'Autorité en profite pour rappeler que la réalisation de statistiques n'est pas une finalité au sens de l'art. 5.1.b) du RGPD (ni des dispositions correspondantes des Titres II et III de la LTD). En réalité, la réalisation de statistiques implique des traitements de données en vue d'une finalité devant être déterminée, explicite et légitime (qui, en l'espèce, est l'évaluation de la loi).

⁶⁵ C.O.C., *Rapport d'activité 2020*, pp. 16 et sv., disponible sur https://www.organedeconrole.be/files/Rapport-dactivit%C3%A9_COC_2020_F.pdf: « nous constatons qu'environ **75,69 % des dossiers traités en 2020** (109 dossiers sur 144) **se sont soldés par un archivage/effacement complet ou partiel des enregistrements effectués par la police dans la BNG**. En comparaison de 2019, ce pourcentage a donc encore augmenté dans des proportions substantielles, de 52 % à 75,69 % (...) ».

Il s'agit ni plus ni moins d'un **chiffre alarmant** qui prouve ce que l'Organe de contrôle observe aussi dans le cadre de ses activités, à savoir que la qualité (l'exactitude et la précision) des banques de données policières laisse encore (trop) à désirer. Ce constat n'est pas innocent : **les citoyens sont** directement ou indirectement **préjudiciés** par des traitements de données incorrects, dépassés ou autrement impropres. **Directement**, parce que le traitement dont le citoyen fait l'objet (fouille, arrestation, approche policière, lien avec les banques de données techniques ANPR, etc.) ne saurait être correct dès lors qu'il repose sur des informations erronées. Et **indirectement**, du fait qu'il est ainsi fait obstacle ou mis un terme à l'accès à certains métiers : les agents de sécurité, les militaires, les détectives privés, les travailleurs d'une centrale nucléaire et autres sont tous jugés purement sur leurs « antécédents policiers » ».

⁶⁶ C.const., arrêt 108/2016 du 14 juillet 2016 (<https://www.const-court.be/public/f/2016/2016-108f.pdf>); CEDH, grande chambre, 4 décembre 2008, S. et Marper c. Royaume Uni, § 103; 18 avril 2013, M.K. c. France, § 35; 17 décembre 2009, B.B. c. France, § 61; 18 septembre 2014, Brunet c. France, §§ 35-40

⁶⁷ Concernant la communication à des services étrangers et donc le traitement ultérieur de ces données par ces services

⁶⁸ Cour constitutionnelle, arrêt du 15 mars 2018, B.18.

⁶⁹ Voy. l'analyse de la proportionnalité

Observations relatives aux CSIL-R

61. L'Autorité constate qu'alors que le commentaire (notamment des art. 31 et 32) contient des références aux CSIL-R, les projets eux-mêmes ne prévoient aucun traitements de données par les CSIL-R⁷⁰. Si le projet entend permettre des traitements de données par les CSIL-R (en ce compris la collecte de données transmises par les TFL et la communication de données aux TFL), il y a lieu de déterminer les éléments essentiels de ces traitements dans le projet de loi. Si telle n'est pas l'intention du demandeur, par souci de clarté, il y a lieu de préciser dans le commentaire que le projet ne constitue pas la base légale des traitements de données par les CSIL-R (et idéalement d'identifier cette base légale⁷¹).
62. En revanche, si l'intention du demandeur est de limiter les traitements de données réalisées par les CSIL-R à des finalités liées à la « prévention sociale » (comme le mentionne le commentaire de l'art. 31), il y a lieu de mentionner expressément dans le projet de loi. En effet, d'une part, les CSIL-R ne travaillent actuellement PAS QUE au niveau de la prévention sociale (puisqu'elles comportent un volet détection précoce des personnes se trouvant dans un processus de radicalisation (ou que des signes permettent de penser qu'elles se trouvent dans un processus de radicalisation))⁷² et, d'autre part, la notion d'« *optique sécuritaire* » des TFL ne permet pas d'exclure une dimension largement préventive (puisque les données traitées ne se limitent pas à des données relatives à des infractions)⁷³.
63. A toutes fins utiles, l'Autorité rappelle que la fonction préventive des CSIL-R⁷⁴ est actuellement précisée dans les travaux préparatoires de la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme⁷⁵ (ci-après « loi CSIL) en ces termes : « *Les CSIL R sont un instrument dans la lutte contre la radicalisation violente du fait qu'elles détectent, de manière précoce, des personnes se trouvant dans un processus de radicalisation et qu'elles peuvent élaborer des trajets de suivi individualisés à leur égard. (...) Alors que la TFL se focalise sur une **approche réactive et répressive** par le biais d'un suivi policier et judiciaire (...), la CSIL R aborde la personne dans un contexte de société inclusive. Cette différence au niveau de l'approche se reflète dans la composition des structures de concertation. (...) La CSIL R est*

⁷⁰ Seul le rapport au Roi concernant l'art. 3 du projet d'AR indique que les « *enfants pourraient (...) éventuellement être abordés dans le CSIL-R, et les services socio-préventifs pourraient initier un accompagnement si nécessaire* »

⁷¹ Les normes contenant les éléments essentiels des traitements ne doivent pas être confondues avec la norme créant les CSIL-R

⁷² Voy. OCAM, Plan R : Note de clarification sur la CSIL-R, décembre 2019 ; F. XAVIER, *L'accroissement du rôle du bourgmestre dans les matières liées à la sécurité, spécialement en ce qui concerne le radicalisme, l'extrémisme violent et le terrorisme*, Rev. dr. communal, 2021/2

⁷³ « *Des personnes qui n'ont commis aucun fait punissable peuvent figurer dans cette banque de données commune qui a une fonction préventive* »

(<https://www.lachambre.be/doc/ccra/pdf/55/ac929.pdf>), p. 23

⁷⁴ Voy. art. 2 de la loi CSIL

⁷⁵ MB 14.09.2018

principalement composée des acteurs sociaux du niveau local. À l'exception de la police locale (Information Officer) qui assure le lien avec la TFL, aucun membre de la TFL ne siège au sein de la CSIL R »⁷⁶. L'Information Officer de la police locale assure quant à lui le partage d'informations entre les TFL et les CSIL R⁷⁷.

Finalités de l'information d' « autres destinataires »

64. En vertu de l'art. 24 du projet de loi, une carte d'information⁷⁸ peut être communiquée « à une autorité ou une institution tierce, qui a le besoin d'en connaître, (...) ». Le commentaire de cette disposition donne l'exemple de la communication de données « à un travailleur social ou à un directeur d'école afin de prévenir un départ d'un jeune en décrochage social vers la Syrie » ou encore le bourgmestre.
65. L'Autorité fait tout d'abord remarquer que le principe d'une communication basée sur le besoin d'en connaître implique une évaluation en fonction des (catégories de) données et non de l'ensemble d'un support (la carte d'information). A noter que l'Autorité s'interroge sur la pertinence de prévoir⁷⁹ une évaluation de la communication à la fois par les services de base ET par deux services qui sont eux-mêmes considérés comme des services de base.
66. Ensuite, l'Autorité s'interroge sur la compatibilité de l'exemple du travailleur social ou le directeur d'école, avec la notion d'« autorité » ou « institution » tierce. L'Autorité estime toutefois que ces destinataires pourraient être visés indirectement, si le destinataire était le responsable du traitement d'une concertation réalisée en CSIL-R (qui, selon l'Autorité, devrait être le bourgmestre). L'art. 24 du projet de loi et son commentaire doivent donc être reformulés.
67. En ce qui concerne le bourgmestre, l'Autorité constate que son information est également régie par l'art. 12 du projet d'arrêté. Toutefois, la disposition de la loi en vertu de laquelle le Roi est habilité à préciser les finalités de cette communication n'apparaît pas clairement. A défaut de baliser clairement le fondement légal et les limites de cette habilitation, ces dispositions seront donc mentionnées dans le projet de loi.

⁷⁶ Doc. parl., Ch., 2017-2018, DOC 54-3209/001, p. 4

⁷⁷ *Ibid.*, p. 8, voy. aussi art. 4 de la loi CSIL

⁷⁸ Il s'agit d'un « *extrait de la fiche de renseignements, contenant les données à caractère personnel et informations, strictement limitées au besoin d'en connaître du destinataire, pour le suivi des entités* » (art. 2, 10° du projet de loi). A noter que le commentaire relatif à la carte d'information distingue erronément les données à caractère personnel de l'évaluation de la menace, des liens avec d'autres entités, les alias et les mesures appliquées, qui sont pourtant également des données à caractère personnel.

⁷⁹ *Une carte d'information peut être communiquée, à une autorité ou une institution tierce, qui a le besoin d'en connaître, après évaluation par le gestionnaire, le responsable opérationnel et les services de base*

68. Par ailleurs, le commentaire de l'art. 24 du projet distingue la communication au bourgmestre (1) par voie du chef de corps, qui « *a pour objectif d'informer le plus rapidement possible le bourgmestre même si les informations disponibles ne sont pas encore complètes* » de celle (2) au moyen de « *la* »⁸⁰ carte d'information « *pour qu'il puisse prendre les mesures qui relèvent de ses compétences* ». L'art. 12 du projet d'arrêté précise que le bourgmestre est destinataire de « *la* » carte d'information relative aux entités « *qui ont établi leur résidence ou domicile dans sa commune, la fréquentent régulièrement ou y organisent régulièrement des activités* », à l'exception des PH qui sont limités à ceux « *dont les effets sont perceptibles dans sa commune ou qui ont établi leur résidence ou leur domicile dans sa commune, la fréquentent régulièrement, y organisent ou y planifient d'organiser une ou plusieurs activités* ». L'art. 12, §2 précise que « *le bourgmestre utilise, après un contact avec le chef de corps de la zone de police qui lui a transmis la carte d'information, les données à caractère personnel et informations émanant de celle-ci dans le cadre de ses compétences légales et sous sa propre responsabilité* ». Le rapport au Roi permet de comprendre que par « *utilisation* », il y a lieu de comprendre le « *partage* » des données et informations « *avec les différents acteurs locaux qui ont besoin d'en connaître* » et que « *le cadre de ses compétences légales* » vise, d'une part, sa compétence « *définie dans la nouvelle loi communale(...) dans le domaine de la prévention en matière de terrorisme* » et d'autre part sa qualité d'« *autorité en matière de police administrative* » en vertu de laquelle « *il doit également être tenu au courant du suivi concret de certaines entités liées à sa commune* ».
69. L'Autorité relève qu'alors que l'art. 12, §2 du projet d'arrêté impose le préalable systématique du contact avec le chef de corps, le rapport au Roi ne l'impose que « *s'il existe un doute quant au fait de mettre en péril une mission opérationnelle* ». Cette disposition (ou le rapport) devra donc être adaptée. A cette occasion, la possibilité de communication « *sous sa responsabilité* » sera précisée de manière à ce que cette disposition ne puisse être interprétée comme une « *clause de limitation de la responsabilité* » des responsables du traitement de la BDC pour avoir communiqué des données à caractère personnel en vue d'un traitement dont les finalités ne seraient pas déterminées, explicites et légitimes. A noter qu'une telle clause serait sans effet, puisque contraire à des normes hiérarchiquement supérieures.
70. Il est donc essentiel de déterminer avec précision la qualité en vertu de laquelle un bourgmestre est susceptible d'être destinataire de données à caractère personnel. Cette détermination a en effet un impact, outre sur la responsabilité de l'autorité à l'origine de la communication (mentionnée ci-avant),

⁸⁰ Cette carte devant pouvoir être modalisée, il est préférable de mentionner « d'une » carte d'information

sur ses compétences, sur sa qualité de responsable du traitement⁸¹ et sur la possibilité d'impliquer ou non les services communaux (au regard des principes de proportionnalité et de minimisation)⁸².

71. Ainsi, si sa qualité d'autorité en matière de police administrative vise une application de l'art. [Art. 133](#), al. 3 NLC, il y a lieu de s'interroger l'absence de distinction entre son rôle de celui des autres autorités administratives que sont le Ministre de l'Intérieur et les gouverneurs (et le Ministre-président). En revanche, si c'est l'autorité du bourgmestre sur la police locale, qui est visée, il y a lieu de se référer aux [Art. 42](#) et [45](#) LPI et de citer également le Collège de police. Par ailleurs, l'Autorité relève que la communication au bourgmestre en sa qualité d'autorité en matière de police administrative a pour seule finalité de « *le tenir au courant du suivi* ». Ce libellé est toutefois incompatible avec la notion d'« *utilisation* » des données prévue à l'art. 12 du projet d'arrêté.
72. En ce qui concerne la compétence du bourgmestre définie dans la nouvelle loi communale, il y a lieu de se référer aux « *mesures de police administratives* »⁸³.
73. L'Autorité s'étonne également de l'absence d'adéquation avec les dispositions relatives aux compétences du bourgmestre en matière de concertation de cas (au sens de l'art. 458ter CP) figurant dans la loi CSIL et les décrets communautaires⁸⁴. Au besoin, le projet sera donc adapté afin de préciser les finalités du traitement au regard des compétences légales⁸⁵ du destinataire.

II.3. Principe de proportionnalité/minimisation des données

74. L'art. 2, 2° du projet de loi modifiant la LCA entend insérer un nouvel alinéa⁸⁶ à l'art. 4 de la LCA en vertu duquel « *en application de la présente loi, il est tenu compte d'un principe directeur du Règlement 2016/679 qui stipule que le traitement des données à caractère personnel devrait être conçu pour*

⁸¹ Sur cette question voy. COC, Avis d'initiative DD200026 du 11 février 2021 concernant la question de savoir qui est le responsable du traitement pour les traitements de données par les services de police dans le cadre de l'exécution de missions policières d'une part et pour les traitements de données en vertu du RGPD d'autre part (https://www.organedeconrole.be/files/DD200026_Responsable_de_Traitements_GPI_F.PDF)

⁸² Et sur la nécessité ou non d'adapter la circulaire du 1^{er} décembre 2006 relative à l'allègement et la simplification de certaines tâches administratives de la police locale

⁸³ Voy. Mercuriale du PG I. de la Serna, La montée en puissance de la répression administrative : recul ou progrès d'une société, 2 septembre 2019, p. 6, ainsi que les références citées (https://www.ommp.be/sites/default/files/u1/mercuriale_2019_mo_0.pdf)

⁸⁴ Voy. le décret flamand du 21 mai 2021 portant l'autorisation des participants flamands et réglant les modalités de participation aux CSIL R

⁸⁵ Pour autant que le législateur ait l'intention d'adopter ce projet, il sera également tenu compte de la concertation de cas prévue par l'art 35 de l'avant-projet de loi « *relative à l'approche administrative communale, à la mise en place d'une enquête d'intégrité communale et portant création d'une Direction chargée de l'Évaluation de l'Intégrité pour les Pouvoirs publics* », rétablissant l'art. 119ter de la Nouvelle Loi communale, Au sujet duquel l'Autorité a rendu l'avis 245/2022 du 21 octobre 2022 (<https://www.autoriteprotectiondonnees.be/publications/avis-n-245-2022.pdf>); voy. également l'avis n° 13/2022 du 18 novembre 2022 rendu par l'Institut fédéral pour la protection et la promotion des droits humains (<https://institutfederaldroitshumains.be/sites/default/files/2022-11/Avis%20IFDH%20Approche%20administrative%20communale.pdf>)

⁸⁶ Reproduisant le 4^{ème} considérant du RGPD

servir l'humanité et que le droit à la protection des données à caractère personnel qui n'est pas un droit absolu doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité »⁸⁷.

75. Dans son arrêt 52/2021, la Cour constitutionnelle a estimé que l'objectif visant à lutter contre le terrorisme et contre la radicalisation correspond incontestablement à un besoin social impérieux⁸⁸.

76. **L'Autorité partage ce constat** et s'attelle ci-après à vérifier si les moyens prévus par le projet sont bien nécessaires et proportionnés pour répondre à ce besoin social. En effet, comme l'a rappelé la Cour constitutionnelle dans son arrêt 110/2022, « *la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige, conformément à la jurisprudence constante de la Cour de justice, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire*⁸⁹. Pour juger du caractère proportionné de mesures relatives au traitement de données à caractère personnel, il convient de tenir compte notamment de leur caractère automatisé, des techniques utilisées, de la précision, de la pertinence et du caractère excessif ou non des données traitées, de l'existence ou de l'absence de mesures qui limitent la durée de conservation des données, de l'existence ou de l'absence d'un système de contrôle indépendant permettant de vérifier si la conservation des données est encore requise, de la présence ou de l'absence de droits de contrôle et de voies de recours suffisants pour les personnes concernées, de la présence ou de l'absence de garanties visant à éviter la stigmatisation des personnes dont les données sont

⁸⁷ Doc. parl., Ch., 2021-2022, DOC 55-2793/001, p. 98; L'Autorité souligne que le 4^{ème} considérant du RGPD (que la disposition précitée reproduit) concerne l'art. 1^{er} du RGPD, auquel se rapportent également les considérants 1 à 3, 9, 10 et 13. Le 3^{ème} paragraphe de l'art. 1^{er} du RGPD dispose que « *la libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel* ». La lecture conjointe de l'ensemble des considérants applicable à l'art. 1^{er} permet de comprendre que l'intention des auteurs était d'éviter que des différences de niveau de protection entre Etats membres empêche « *le libre flux de ces données dans l'ensemble de l'Union* ». Les dispositions du RGPD respectent « *tous les droits fondamentaux* » (consid. 4), mais permet aux législateurs nationaux de préciser les règles du RGPD (consid. 10). En d'autres termes, les règles du RGPD assurent l'harmonisation minimale appelées à assurer la libre circulation des données et, si le RGPD permet aux législateurs nationaux d'encadrer plus strictement certains traitements, la hiérarchie des normes s'oppose à ce qu'un législateur national adopte une norme dérogeant aux dispositions du RGPD. A l'occasion de son arrêt 110/2022, la Cour constitutionnelle a rappelé que « *la proposition qui a précédé l'adoption de l'article 22 de la Constitution insistait sur « la protection de la personne, la reconnaissance de son identité, l'importance de son épanouissement et celui de sa famille », et elle soulignait la nécessité de protéger la vie privée et familiale « des risques d'ingérence que peuvent constituer, notamment par le biais de la modernisation constante des techniques de l'information, les mesures d'investigation, d'enquête et de contrôle menées par les pouvoirs publics et organismes privés, dans l'accomplissement de leurs fonctions ou de leurs activités » (Doc. parl., Sénat, S.E. 1991-1992, n° 100-4/2°, p. 3). Cette proposition indiquait également que le législateur « ne pourrait en aucun cas vider de sa substance le droit au respect de la vie privée et familiale, sous peine d'enfreindre la règle constitutionnelle, en plus des règles internationales » (ibid.) » (Arrêt du 22 septembre 2022, B.7.4., p. 27 (<https://www.const-court.be/public/f/2022/2022-110f.pdf>)).*

La condition de nécessité et le principe de proportionnalité figurent également au considérant 39 du RGPD qui se rapporte à l'art. 5.1.c) du RGPD (en ce sens voy. CJUE, 22 juin 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraphe 110 et la jurisprudence citée et CJUE, 11 décembre 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, EU:C:2019:1064, paragraphe 48).

⁸⁸ Arrêt du 1^{er} avril 2021, B.13, p. 29 (<https://www.const-court.be/public/f/2021/2021-052f.pdf>)

⁸⁹ CJUE, 16 décembre 2008, C-73/07, *Satakunnan Markkinapörssi et Satamedia*, point 56; 8 avril 2014, C-293/12 et C-594/12, *Digital Rights Ireland e.a.*, points 51 et 52; 6 octobre 2015, C-362/14, *Schrems*, point 92, 21 décembre 2016, C-203/15 et C-698/15, *Tele2 Sverige et Watson e.a.*, points 96 et 103; 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, point 130

*traitées et de la présence ou de l'absence de garanties visant à éviter l'usage inapproprié et abusif, par les services publics, des données à caractère personnel traitées*⁹⁰ »⁹¹.

77. L'Autorité rappelle que la multiplication des services impliqués⁹² a pour effet (et même pour objet) d'augmenter la quantité de données à caractère personnel traitées et de permettre la combinaison de ces données, engendrant par voie de conséquence une aggravation de l'ingérence dans les droits et libertés des personnes concernées⁹³.
78. De plus, dans la mesure où les dispositions relatives à la BDC ont été intégrées dans la LFP depuis 2016 et ont depuis lors été abondamment critiquées par la doctrine autorisée⁹⁴, il ne peut être admis de reproduire ces dispositions sans intégrer dans le commentaire de l'article concerné une évaluation empirique de l'effet de ces mesures⁹⁵ sur la prévention du terrorisme et du radicalisme violent et donc du respect par les dispositions concernées de la condition de nécessité et du principe de proportionnalité. En effet, comme le rappelle un récent rapport au Haut-Commissaire des Nations-Unies aux Droits humains, s'inquiétant des menaces que la surveillance fait peser sur les démocraties : « *les Etats négligent trop souvent de démontrer l'efficacité des systèmes de surveillance qu'ils mettent en œuvre* »⁹⁶.
79. L'Autorité estime donc que l'exposé des motifs du projet doit contenir une justification du caractère nécessaire et proportionné de la participation de chacun des nouveaux partenaires ainsi que du maintien de chacun des services participant actuellement. Cette justification devra démontrer (sur base

⁹⁰ Arrêt n° 108/2016 du 14 juillet 2016, B.12.2; arrêt n° 29/2018 du 15 mars 2018, B.14.4; arrêt n° 27/2020 du 20 février 2020, B.8.3; CEDH, grande chambre, 4 mai 2000, Rotaru c. Roumanie, § 59; décision, 29 juin 2006, Weber et Saravia c. Allemagne, § 135; 28 avril 2009, K.H. e.a. c. Slovaquie, §§ 60-69; grande chambre, 4 décembre 2008, S. et Marper c. Royaume-Uni, §§ 101-103, 119, 122 et 124; 18 avril 2013, M.K. c. France, §§ 37 et 42-44; 18 septembre 2014, Brunet c. France, §§ 35-37; 12 janvier 2016, Szabó et Vissy c. Hongrie, § 68; CJUE, grande chambre, 8 avril 2014, C-293/12, Digital Rights Ireland Ltd et C-594/12, Kärntner Landesregierung e.a., points 56-66

⁹¹ Arrêt du 22 septembre 2022, B.22, pp. 57-58 (<https://www.const-court.be/public/f/2022/2022-110f.pdf>); L'Autorité ajoute que dans l'affaire *Asociația de Proprietari bloc M5A-ScaraA*, la Cour de justice a précisé que la condition de nécessité devait être examinée en conjonction avec le principe de minimisation consacré à l'art. 5.1.c) du RGPD (*op. cit.*, §48); Voy. également CJUE, 5 avril 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, paragraphe 52 et 11 décembre 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, EU:C:2019:1064, paragraphe 57

⁹² Tant dans ceux ayant accès à la BDC que ceux qui participent aux concertations en TFL

⁹³ En ce sens, voy. Opinion 1/15 (*EU-Canada PNR Agreement*) du 26 juillet 2017, EU:C:2017:592, paragraphe 128

⁹⁴ Voy. notamment G. Vermeulen and S. De Coensel, "Gemeenschappelijke gegevensbanken in de strijd tegen het terrorisme: noodzakelijke maar te brede sleepnetten," *POLITIE EN RECHT*, vol. 4, no. 4, pp. 164-177, 2021 (<http://hdl.handle.net/1854/LU-8733193>)

⁹⁵ Notamment basées sur les statistiques de la criminalité (les statistiques policières de 2000 au 3^{ème} trimestre 2022, sont consultables via le lien suivant :

https://www.police.be/statistiques/sites/statspol/files/statistics_files_upload/Criminaliteit%20-%20Criminaliteit/crimi_fr/01_Rapports/01_F%C3%A9d%C3%A9ral/rapport_2022_trim3_nat_belgique_fr.pdf.

⁹⁶ Rapport du 4 août 2022, The right to privacy in the digital age, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement>, point 54

de critères aussi objectifs que possible⁹⁷) que l'accroissement de l'ingérence résultant des dispositions du projet répond à un besoin de renforcement des mesures de lutte contre le terrorisme et contre la radicalisation.

80. Lors de cette démonstration, le caractère proportionné de la communication de données aux services participants sera évalué par rapport à la possibilité d'atteindre la finalité visée par une communication de certaines données par l'un des services de base seul (par exemple sous forme de rapport de police ou d'extrait de l'analyse de la menace réalisée par l'OCAM).
81. Afin d'éviter qu'à l'avenir il puisse être reproché à la Belgique de ne pas démontrer l'efficacité des systèmes de surveillance qu'ils mettent en œuvre, l'Autorité estime qu'il convient de prévoir (à l'art. 4 du projet) que des statistiques seront réalisées aux **fins de la publication d'un rapport d'évaluation** (selon une périodicité à déterminer dans le projet, mais qui ne devrait pas être inférieur à tous les 3 ans) portant sur l'efficacité des moyens de traitements mis en œuvre et des autorités impliquées par la loi en projet et son arrêté d'exécution par rapport aux finalités pour lesquelles les données ont été enregistrées dans la BDC.
82. La démonstration du caractère nécessaire et proportionné de la communication devra également porter sur les modalités de cette communication. A cette occasion, il conviendra de démontrer en quoi la centralisation systématique et exclusive des données au niveau de la BDC est davantage susceptible de rencontrer la finalité visée qu'un accès modalisé en fonction des finalités poursuivies, dans le cadre d'un système de banque-carrefour, qu'une simple notification « *push* » aux autres services intéressés

⁹⁷ L'Autorité précise que la justification des ingérences répondant à un impératif sécuritaire est appréciée au regard du contexte prévalant au moment de l'adoption de la norme. Par conséquent, l'évaluation du caractère nécessaire et proportionné de l'extension d'une mesure doit s'accompagner de la mention dans l'exposé des motifs du projet des éléments de contexte (perpétration d'actes terroristes, niveau de la menace, etc.) entourant la création de la BDC et l'extension des traitements à d'autres entités (pour des éléments de contexte, voy. C. Debrulle, Lutte anti-terroriste ou combat liberticide ? Évaluation en 2016, JDJ n° 360 - décembre 2016, pp. 10 et sv. (<https://www.liquedh.be/wp-content/uploads/2016/12/jdj-b360-12.16%20article%20claudie%20debrulle.pdf>); voy. également M. Moucheron, « Délit politique et terrorisme en Belgique : du noble au vil », Cultures & Conflits [En ligne], 61 | printemps 2006, mis en ligne le 17 mai 2006 (<https://journals.openedition.org/conflits/pdf/2038>); C. Thomas, « L'organisation fédérale de la lutte antiterroriste en Belgique », Courrier hebdomadaire du CRISP, 2020/18-19 (n°2463-2464), pp. 5-66 (<https://www.cairn.info/revue-courrier-hebdomadaire-du-crisp-2020-18-page-5.htm#re289no289>); W. VAN LAETHEM, Het Coördinatieorgaan voor de dreigingsanalyse: Een punctuele analyse, Vigiles, 2007/4 (<https://bib.kuleuven.be/rbib/collectie/archieven/vigiles/2007-4-109-127.pdf>); M. Van Hoey, De Belgische gecoördineerde analyse van de dreiging, van de actie en van de informatiefloed: van AGG over OCAD naar (de toekomst van) het 'Actieplan Radicalisme', Panopticon, Jaargang I Volume 41 » Issue 3., 30 mai 2020 (<http://www.maklu-online.eu/nl/tijdschrift/panopticon/jaargang-i-volume-41/issue-3-mei-juni-2020/de-belgische-gecoördineerde-analyse-van-de-dreiging/pdf/>). Par ailleurs, la Cour de justice estime qu'« *il convient cependant de souligner que le manque de ressources allouées aux autorités publiques ne saurait en aucun cas constituer un motif légitime permettant de justifier une atteinte aux droits fondamentaux garantis par la Charte* » (CJUE, 1^{er} août 2022, C-184/20, OT c. Vyriausioji tarnybinės etikos komisija, §89). Il en résulte que qu'idéalement, il conviendrait également de démontrer que les mesures envisagées n'entendent pas compenser un désinvestissement dans les services de police et de sécurité (pour des éléments de contexte sur ce point, voy. le rapport d'évaluation de la réforme de la police, point 4.1.11., pp. 40 et sv. (<https://www.police.be/5998/sites/5998/files/downloads/cfp-adv-2009-05-29-f.pdf>); voy. également le volet « personnel » du rapport annuel 2021 de la Police Fédérale qui fait état de la stabilité du déficit du personnel opérationnel (<https://rapportannuel.policefederale.be/organisation/notre-personnel/>) alors que le 3^{ème} rapport de la commission attentats comporte également une recommandation visant à ce que « *les efforts nécessaires soient consentis de manière à ce que tous les services disposent de moyens suffisants, surtout après l'élargissement de l'éventail de leurs tâches* » (op. cit., p. 133).

ou qu'une communication d'informations, effectuée par la direction d'un service à son (ou ses) homologue(s) concernés (du moins pour les cas les plus graves)⁹⁸.

L'affaire Conings et l'obligation pour la TFL de parcourir une liste de mesures pouvant être prises (chapitre 3 du projet de loi)

83. L'art. 31 du projet de loi dispose qu'« *en vue d'assurer l'enrichissement des données à caractère personnel et informations relatives aux entités ainsi que le suivi et la prise de mesures à l'égard des entités validées dans la banque de données commune T.E.R., des données à caractère personnel et des informations enregistrées dans la banque de données commune T.E.R. ainsi que d'autres données à caractère personnel et informations pertinentes, y compris les informations classifiées (...), sont échangées au sein d'une ou plusieurs [TFL] créées auprès de chaque arrondissement judiciaire (...)* ».

84. Comme indiqué *supra*⁹⁹, les TFL fonctionnent depuis longtemps (en dehors d'un cadre légal) et le projet de loi entend donc :

- leur conférer une assise légale¹⁰⁰ ;
- déterminer leur finalité spécifique, à savoir alimenter la BDC, suivre et prendre des mesures (art. 31) ;
- étendre leur composition à l'OE et prévoir la possibilité d'inviter « *d'autres services, organes ou instances en raison de la contribution qu'ils peuvent apporter par leur fonction ou leurs compétences à un suivi ciblé et individualisé de l'entité* » (art. 32, §1^{er}) ;
- déterminer ses missions (tout en habilitant le Roi à les étendre)¹⁰¹ (art. 32, §2) ;
- prévoir une concertation obligatoire sur l'opportunité de prendre ou de lever des mesures (énumérées de manière non-exhaustive à l'art. 33, §2)¹⁰² dès la validation ou « *lorsque des nouvelles données à caractère personnel et informations (...) peuvent entraîner un changement de mesures (...)* » (art.33, §1^{er}, al. 2) ; et
- mettre en œuvre une « *approche proactive* »¹⁰³ (art. 33, §1^{er}, al. 3).

⁹⁸ Et de démontrer que le projet impose aux solutions technologiques de s'adapter aux normes (s'inscrivant ce faisant dans une démarche respectueuse de l'Etat de droit) et non pas qu'à l'inverse, il occasionne une ingérence évitable dans les droits et libertés des personnes concernées (par exemple en diluant la responsabilité du traitement ou en prévoyant des communications de données allant au-delà de ce qui est nécessaire) pour s'adapter au fonctionnement d'une solution technologique existante

⁹⁹ Lors de l'analyse des finalités des TFL

¹⁰⁰ Insuffisante au regard du principe de légalité, comme il a été démontré *supra*

¹⁰¹ Habilitation critiquable au regard du principe de légalité (voy. *supra*)

¹⁰² Il s'agit « notamment » du signalement, de mesures liées à la possibilité d'exercer la profession de détective privé, du retrait d'habilitations, attestations et avis de sécurité, de mesures relevant de la compétence du service d'information et de recherche sociale du SPF Emploi (telles qu'une enquête sociale), d'enquêtes financières par la CTIF, de mesures relevant de la compétence de l'ONEm ou de ses homologues régionaux, de mesures en matière d'accès au territoire, de séjour, d'établissement et d'éloignement des étrangers, du refus, du retrait ou de l'invalidation de passeports ou de titres de voyages ou de documents d'identité, de l'inscription ou de la radiation d'office des registres de la population, du gel des avoirs, du suivi policier ou par les services de renseignement et le suivi des médias sociaux de l'entité (dont le projet ne précise pas quelle autorité exécutera cette mesure).

¹⁰³ C'est-à-dire la transmission du résultat de la concertation aux autorités compétentes pour prendre les mesures

85. Le commentaire du chapitre 3 du projet de loi précise que le projet¹⁰⁴ entend favoriser et optimiser davantage l'échange et la communication entre les différents services compétents en matière de terrorisme-extrémisme, dont l'importance a été réaffirmée par l'affaire Conings. L'Autorité présume qu'en se référant expressément à une affaire tragique et récente, le demandeur entend démontrer que l'accroissement de l'ingérence¹⁰⁵ prévue par les dispositions en projet, permettra effectivement d'éviter que de tels faits se reproduisent, qu'il ne serait pas possible d'atteindre l'objectif recherché au moyen d'une mesure moins intrusive pour le droit au respect de la vie privée ou le droit à la protection des données à caractère personnel et qu'il existe un équilibre entre l'ingérence dans le droit au respect de la vie privée et à la protection des données à caractère personnel et l'objectif¹⁰⁶ poursuivi.
86. L'Autorité précise tout d'abord qu'une description succincte de l'affaire et à l'établissement d'un lien entre cette affaire et l'importance de la communication dont il est simplement mentionné qu'elle s'en serait trouvée réaffirmée, ne peut être considérée comme une démonstration du caractère nécessaire et proportionné de l'ingérence.
87. Toutefois, afin de conseiller au mieux le demandeur quant aux éléments susceptibles d'être invoqués en appui de cette démonstration, l'Autorité a consulté le rapport d'audition du général-major Philippe Boucké (à la tête du SGRS depuis le 18 septembre 2020), dans le cadre de l'affaire Jürgen Conings, devant la Commission de la Défense de la Chambre¹⁰⁷. Il en ressort principalement que les flux de communications dont un besoin de renforcement a été identifié concernent la communication interne (le SGRS connaissait des tensions interpersonnelles internes jusqu'à peu de temps avant les incidents)¹⁰⁸ et avec des partenaires nommément cités « *(Sûreté de l'État, OCAM, FedPol)* »¹⁰⁹. Le besoin de communication des données avec d'autres partenaires n'est donc, ni exprimé, ni démontré dans le rapport d'audition relatif à cette affaire.
88. En revanche, ce rapport d'audition permet d'identifier les mesures susceptibles de prévenir efficacement les faits qui se sont produits. Il y est notamment indiqué que l'habilitation de sécurité n'avait pas été renouvelée en 2020, mais que le règlement d'accès aux armes n'attache pas de conséquences à la perte d'une habilitation de sécurité¹¹⁰ et que si le SGRS n'a pas pu envoyer de représentant à la TFL le jour où le niveau de la menace concernant l'intéressé a été augmenté par

¹⁰⁴ Qui entend prévoir l'échange de données au sujet d'une entité, au sein d'une plateforme de concertation (la TFL) et que la TFL se concertent, dès la validation d'une entité dans la BDC, au sujet d'éventuelles mesures à prendre

¹⁰⁵ Résultant de l'inclusion d'acteurs ne relevant pas de la chaîne pénale et de sécurité (en ce compris l'OE) dans les autorités tenues de communiquer et de se voir communiquer des données, relatives aux entités, dans le cadre des concertations en TFL

¹⁰⁶ Effectivement atteignable

¹⁰⁷ Doc. Parl. Ch., 23 septembre 2021, 55-2206/001, pp.7 et sv.

¹⁰⁸ *Ibidem*, p. 12

¹⁰⁹ *Ibidem*, p. 14

¹¹⁰ « A noter qu'une habilitation de sécurité permet à un membre de la Défense d'accéder à des informations classifiées, s'il a le besoin d'en connaître dans le cadre de sa fonction, ou à des zones classifiées. Il n'est nullement question ici d'avoir ou de ne pas avoir accès à des armes et dépôts de munitions », *Ibidem*, p. 10

l'OCAM, c'est en raison du (1) manque de personnel¹¹¹ et de (2) la nécessité de donner la priorité à une autre menace¹¹², dès lors que tous les éléments disponibles, y inclus ceux venant de la Police et du monde judiciaire, indiquaient qu'il y avait peu ou pas d'éléments contre Jürgen Conings à ce moment précis¹¹³.

89. L'Autorité en conclut que le caractère nécessaire et proportionné de la participation de l'OE aux TFL n'est pas démontrée dans l'état actuel du projet et ne semble pas démontrable à l'aide du cas cité en commentaire. A l'inverse, la nécessité de la communication aux services en charge de l'accès aux armes¹¹⁴ (au sein des différentes autorités dont l'exercice des fonctions par leurs agents respectifs implique à accès à des armes) du retrait d'une habilitation de sécurité de l'un de leurs agents, mais surtout la communication du résultat négatif d'un rapport faisant suite à un examen psychologique auquel cette catégorie d'agents sont vraisemblablement périodiquement soumis, ressort très clairement de l'exemple cité.
90. Le caractère nécessaire et proportionné du fait de différer la prise d'une mesure en la soumettant à une concertation préalable (voy. par exemple l'art. 33, §2, 4° du projet de loi en ce qui concerne le retrait d'une habilitation de sécurité) et donc à une communication réciproque de données entre services disposant chacun de compétences propres en la matière, n'est pas non plus démontré dans l'état actuel du projet. Il convient donc de distinguer la concertation préalable obligatoire (qui est certainement justifiée vis-à-vis du parquet) de la communication en temps réel ou a posteriori de l'information relative à la prise d'une mesure, avec les services disposant de données à l'égard de l'intéressé.
91. Par ailleurs, les services susceptibles d'être invités (qui seront appelés à transmettre ou à collecter des données en participant aux TFL) doivent à tout le moins être déterminables. Le commentaire de l'art. 32 se réfère sur ce point à « *leurs compétences ou fonctions* » et à leur caractère « *fiable* ». Ces éléments ne sont pas de nature à permettre à une personne concernée que le traitement de ses données par ce service invité soit nécessaire et proportionné à la finalité poursuivie. Les critères seront donc détaillés dans le commentaire de l'art. 32. En tout état de cause, en ce qui concerne les services ne relevant pas de la chaîne pénale et de sécurité ou à l'égard desquels la participation se limite à la communication des informations nécessaires pour leur permettre de prendre une mesure, il convient de prévoir que la personne concernée doit déjà être « *connue* » du service participant et que ce service doit disposer d'informations susceptibles d'être « *utiles* » à son sujet.

¹¹¹ « *Le détachement local ne comptait que deux officiers à l'époque – entretemps, il avait fait renforcer l'équipe – et que l'un d'eux était en congé de maternité. Le second officier absent avait deux réunions à son agenda ce jour-là* », Ibidem, p. 11 ; « *La loi du 30 novembre 1998 définit les rôles, les fonctions et les tâches des services de renseignement et de sécurité. Le SGRS a beaucoup de missions légales, pas seulement celles mentionnées dans la loi organique. Le Service a listé toutes ses obligations, une liste qui compte 21 pages* », Ibidem, p. 13

¹¹² Qualifié de dossier brûlant, Ibidem, p. 14

¹¹³ En 2019, « *la Défense a, par ailleurs, réagi en portant plainte auprès de la police. Le parquet a classé le dossier sans suite* », Ibidem, pp. 9 et 11

¹¹⁴ Aux fins d'interdire un accès aux armes et munitions à l'intéressé

92. A l'occasion de la reformulation de l'art. 31 du projet de loi¹¹⁵, il conviendra par ailleurs de préciser la **notion d'« échange » de données**. En effet, celle-ci ne correspond pas à proprement parler à un traitement de données et il n'est donc pas possible d'en déduire les conditions d'un traitement relatif à ces données. Il sera avant tout veillé à démontrer le caractère nécessaire et proportionné de l'aspect « réciprocité » que la notion d'échange attache à la communication des données. En d'autres termes, il sera démontré (dans le commentaire du chapitre 3), pour chacun des participants et invités potentiels et pour chaque catégorie de donnée, que la communication de données¹¹⁶ (que le participant n'a pas déjà collecté en vertu de ses propres missions) est bien nécessaire et proportionné. A la lecture de cette démonstration, il devra par exemple être possible de déterminer (1) quels sont les critères pour considérer qu'une mesure d'invalidation de passeport doit être « concertée » (et non adoptée unilatéralement par l'autorité compétente), (2) quelles sont les autorités dont il est justifié qu'elles participent (ou soient invitées) à une telle concertation (plutôt que de recevoir le résultat de la concertation si elles sont l'autorité compétente pour prendre la mesure et (3) les Affaires consulaires (et/ou d'autres participants étrangers à la chaîne pénale et de sécurité) doivent-elles uniquement être invitées à partager leurs données au sujet de l'entité discutée (ou faire part de la faisabilité pour elles de prendre une mesure¹¹⁷) ou doivent-ils également prendre connaissance des données détenues par les autres autorités membres de la chaîne pénale et de sécurité¹¹⁸ ?

Catégories de données

93. Le projet de loi prévoit le traitement des données à caractère personnel qu'il énumère à l'art. 6, §2. Toutefois, en énumérant les données susceptibles d'être traitées « *dans la banque de données* », le projet ne permet pas de comprendre lesquelles de ces données sont susceptibles d'être traitées par quel service (et encore moins d'en évaluer le caractère nécessaire et proportionné).
94. Or, comme il a été dit ci-avant¹¹⁹, il n'est ni nécessaire, ni proportionné que le service des cultes et de la laïcité soit en mesure de savoir si un EPV non religieux est enregistré en BDC. Dans le même ordre d'idée, dans l'état actuel du projet, la Trésorerie ne doit pas être en mesure de consulter les données de santé d'une entité dont les avoirs doivent être gelés, les établissements pénitentiaires ne doivent pas pouvoir traiter les données relatives à des personnes qui ne sont pas privées de liberté et l'Office des étrangers ne doit pas intervenir dans le traitement d'entités qui ne disposent que de la seule nationalité belge.

¹¹⁵ En ce qui concerne la nécessité de la reformulation au regard du principe de limitation des finalités, voy. *supra*

¹¹⁶ Mais aussi la présence de chacun de ces participants à la TFL

¹¹⁷ Par exemple l'annulation d'un document de voyage

¹¹⁸ L'Autorité estimant que dans l'état actuel des éléments en sa possession, il convient d'exclure cette seconde possibilité

¹¹⁹ Dans l'analyse des finalités

95. Par conséquent, l'Autorité estime qu'il y a lieu de reformuler l'art. 6 en distinguant – pour chacun des services partenaires - les catégories de données dont ces services disposent et sont habilités à communiquer en vertu de ce projet « *dans le respect du besoin d'en connaître* » des autres services (surtout des services participants), des données communiquées par d'autres participants, en réunion de concertation, dont les autres services participants ont la possibilité de prendre connaissance. A cette occasion, il conviendra de démontrer que le projet impose aux solutions technologiques de s'adapter aux normes (s'inscrivant ce faisant dans une démarche respectueuse de respect de l'Etat de droit) et non pas, qu'à l'inverse, il occasionne une ingérence évitable dans les droits et libertés des personnes concernées¹²⁰ pour s'adapter au fonctionnement d'une solution technologique existante.
96. L'Autorité rappelle par ailleurs que s'agissant de données détenues, au moins partiellement, par d'autres services, le principe de minimisation requiert qu'à chaque fois que la finalité pourra être atteinte par la communication de données d'un seul service (par exemple un extrait de l'analyse de la menace de l'OCAM ou un rapport de la police locale), il soit procédé de la sorte.
97. En ce qui concerne les **catégories de données** elles-mêmes, tout en constatant que le commentaire de l'art. 6 permet une assez bonne compréhension des données qui sont susceptibles d'être traitées, l'Autorité rappelle que, comme indiqué ci-avant, dans la mesure où la loi créant les BDC date de 2016, il ne peut être admis d'en transférer les dispositions sans intégrer dans le commentaire de l'article concerné une évaluation empirique du respect par la disposition concernée de la condition de nécessité et du principe de proportionnalité. Il en résulte, en ce qui concerne les catégories de données traitées, la nécessité de démontrer, sur base d'éléments factuels et objectifs, l'efficacité du traitement de données à caractère personnel envisagé pour atteindre l'objectif recherché et que les avantages qui découlent du traitement de données en question doivent donc être plus importants que les inconvénients qu'il génère pour les personnes concernées.
98. Comme à chaque fois que des données issues des banques de données policières sont susceptibles d'être traitées, l'Autorité souligne que les responsables du traitement doivent être invités à consacrer une attention toute particulière au caractère exact à jour des données qu'ils traitent, conformément à l'article 5.1.d), du RGPD. En effet, les faits concernés pourront être contestés dès lors qu'ils ne seront pas nécessairement (définitivement) établis. Par conséquent, l'Autorité estime qu'il convient de prévoir que de telles données ne pourront être traitées, du moins par les services partenaires, que pour autant que leur caractère exact ait pu être établi par le biais d'un « *flux retour justice* » (sur le modèle de celui prévu à l'article 646 du code d'instruction criminelle¹²¹).

¹²⁰ Par exemple en diluant la responsabilité du traitement ou en prévoyant des communications de données allant au-delà de ce qui est nécessaire

¹²¹ Les catégories d'informations extraites de décisions coulées en force de chose jugée prise par un tribunal correctionnel, une cour d'assises ou une cour d'appel et qui sont susceptibles de modifier celles enregistrées dans la banque de données nationale générale visée à l'article 44/7 de la loi du 5 août 1992 sur la fonction de police, dénommée ci-après BNG, sont communiquées endéans les trente jours à la police, selon les modalités définies par le Roi, par arrêté délibéré en Conseil des ministres. Les catégories d'informations extraites de décisions de non-lieu des juridictions d'instructions qui sont susceptibles de modifier

99. En ce qui concerne le traitement (notamment par interconnexion) des données issues du casier judiciaire des personnes concernées, il convient de préciser – dans un souci de respect du principe de proportionnalité – que l'évocation de condamnations mineures, étrangères aux infractions terroristes visées au titre *I ter* du Livre II du Code pénal, voire très anciennes¹²² ne doivent pas être traitées, du moins par les services partenaires.
100. En ce qui concerne la notion de « *données relatives à la santé* », l'Autorité souligne que le fait de retirer les dispositions relatives à la BDC, de la LFP, est susceptible de conduire à oublier que les services de police ne peuvent eux-mêmes traiter « *les données relatives à la santé (...) uniquement dans le but de comprendre le contexte lié à la personne concernée, ainsi que pour assurer la sécurité et protéger la santé de toute personne susceptible d'entrer en contact avec les personnes concernées dans le cadre de l'intervention policière. Lorsque des données relatives à la santé sont traitées, il est mentionné si ces données proviennent ou non de professionnels de soins de la santé* »¹²³. Il serait difficilement justifiable de permettre aux autres services de traiter toute donnée de santé. Par conséquent, il y a lieu de mentionner cette disposition dans le projet. L'Autorité estime en outre qu'il convient de rappeler dans le commentaire de l'art. 6 que le traitement des données relatives à la santé ne se confond pas avec la communication d'un dossier médical à laquelle les art. 9 et 10 de la loi du 22 août 2002 relative aux droits du patient¹²⁴ continuent à s'appliquer.
101. Le caractère nécessaire et proportionné du traitement des données relatives aux opinions politiques et aux convictions religieuses ou philosophiques, par chacun des services susceptible d'en prendre connaissance, devra également être démontré dans le commentaire de l'art. 6. Une telle démonstration devra conduire à exclure le traitement des données relatives à ces convictions lorsqu'elle seront manifestement inutiles à la finalité générale du projet ou aux missions des services susceptibles d'accéder à la BDC ou d'être invités à participer à une TFL. La démonstration susmentionnée permettra également de **déterminer** si les convictions philosophiques sont (erronément) mentionnées en raison du fait qu'elles sont énoncées conjointement dans de nombreuses dispositions (dont l'art. 9.1. du RGPD) ou **si certaines convictions philosophiques doivent effectivement laisser craindre une radicalisation violente**. Dans le premier cas, la mention de ces données devra bien entendu être omise du projet.

celles enregistrées en BNG sont communiquées endéans les trente jours à la police, selon les modalités définies par le Roi, par arrêté délibéré en Conseil des ministres.

Les catégories d'informations extraites de décisions de classement sans suite pour charge insuffisante ou pour absence d'infraction, prises par le ministère public qui sont susceptibles de modifier celles enregistrées en BNG sont communiquées endéans les trente jours à la police, selon les modalités définies par le Roi, par arrêté délibéré en Conseil des ministres.

¹²² Sur cette question voy. V. De Greef, « *Surveiller et punir... Les personnes condamnées par le casier judiciaire* », Le casier judiciaire. Approches critiques et perspectives comparées, sous la dir. de V. De Greef et J. Pieret, Bruxelles, Larcier, coll. Crimen, 2011, pp. 21-39

¹²³ voy. l'art. 44/1, §3, 2° LFP inséré par la loi du 22 mai 2019 ; La même disposition prévoit en outre que « *le traitement de données relatives à la santé visé dans cet article n'a jamais pour conséquence de contraindre les personnes concernées à se soumettre à des examens médicaux* ».

¹²⁴ MB 26.09.2002

102. De manière générale, le respect du « *besoin d'en connaître* » des autorités participantes implique une que le projet comporte une description des mesures techniques et organisationnelles devant être prises (le cas échéant, via une habilitation au Gouvernement) visant à garantir que des données communiquées par le service compétent dans le cadre d'une finalité liée à la prévention du terrorisme, ne puissent pas être traitées à d'autres fins par d'autres autorités.

Catégories de données traitées par les « autres destinataires »

103. L'Autorité invite également le demandeur à préciser dans le commentaire des art. 24 qu'il ne s'agit en aucun cas de permettre aux « *autres destinataires* » de la carte d'information de se prévaloir de cette disposition pour « *enquêter* » (c'est-à-dire d'étendre les catégories de données à caractère personnel qu'elles sont habilitées à collecter), ni de consolider les données dont ils disposent au sujet des « *entités* », grâce à des informations communiquées par les autres participants, mais qui seraient irrelevantes pour leurs propres finalités. Pour reprendre l'exemple du commentaire au sujet du directeur d'école à qui des informations servaient communiquées afin de prévenir un départ en zone de conflit djihadiste d'un jeune en décrochage, il ne saurait être question de permettre à ce chef d'établissement, d'enregistrer des données relatives aux convictions politiques, des données policières ou toute autre catégorie de donnée relative aux élèves fréquentant son établissements qui ne seraient pas nécessaires à la réalisation des finalités figurant dans les normes organisant l'enseignement dans la communauté concernée. Au vu du risque de dérives, l'Autorité invite le demandeur à considérer d'illustrer cette possibilité de communication de cartes d'informations via les CSIL tout en faisant référence, dans le commentaire, au cadre légal qui les concerne.

Personnes concernées

104. Tout en rappelant ses précédents avis sur la question, l'Autorité s'en remet au COC et au Comité R en ce qui concerne l'évaluation du caractère nécessaire et proportionné du traitement des données à caractère personnel des « *entités* » visées par le projet. L'Autorité estime cependant que le caractère nécessaire et proportionné du traitement des données à caractère personnel de ces entités, doit être démontré service par service.

Cas particulier : les enfants mineurs d'entités

105. L'art. 3 du projet d'AR exécute l'article 6, § 2, alinéa 1er, 1°, 1), b) du projet de loi et prévoit l'enregistrement des données d'identification des enfants biologiques ou adoptés d'un FTF qui s'est rendu dans une zone de conflit djihadiste ou qui sont en route vers la Belgique ou sont revenus en Belgique après s'être rendus dans une zone de conflit djihadiste enregistrée dans la BDC, **âgés de 0 à 18 ans**. Le rapport au Roi précise que la finalité de cet enregistrement est de « *garantir un aperçu des enfants qui séjournent ou ont séjourné dans une zone de combat djihadiste, dans le but d'assurer*

*le suivi nécessaire si ces enfants venaient à revenir en Belgique »¹²⁵ et « connaître leur identité permettra en outre d'assurer leur suivi une fois qu'ils seront de retour dans notre pays après leur séjour dans une zone de conflit djihadiste »¹²⁶. L'Autorité considère que le traitement des données à caractère personnel de ces mineurs – dont elle ne nie pas l'intérêt pour des finalités liées aux missions des services de renseignement – outrepassa de loin les finalités de l'enregistrement dans une banque de données accessible à des services dont les missions sont étrangères à ces finalités. Ce traitement de données d'enfants d'entités « *au cas où* » - qui ne doit pas être confondue avec la situation où le mineur est lui-même une entité¹²⁷ - ne peut donc être effectué par aucun des services relevant de la compétence de l'Autorité.*

106. L'Autorité rappelle au passage que l'existence d'une banque de données n'implique pas que toutes les communications entre deux services concernés par la BDC doivent nécessairement passer par cette voie. Ainsi, si l'Office des Etrangers ou les Affaires Consulaires sont avertis d'un projet de voyage ou si l'un de ces mineurs est identifié à un poste frontière, la consultation des services de renseignement (et la délivrance éventuelle d'un avis négatif) peut parfaitement s'envisager sans que les services précités soient obligés de consulter les données relatives aux parents de l'intéressé. Compte tenu de la justification de certaines dispositions en projet, en décider autrement est susceptible d'aboutir à ce que ce type de données à caractère personnel finisse même par être communiqué à des professionnels de la santé ou à des directeurs d'école¹²⁸.

II.4. Responsables du traitement

107. Sur le plan de la désignation des responsables du traitement, l'Autorité rappelle sa pratique d'avis constante selon laquelle une autorité publique est en principe responsable du traitement de données nécessaire à la mise en œuvre de la mission d'intérêt public qui lui incombe, ou qui relève de l'autorité publique dont elle est investie, en vertu de la législation concernée¹²⁹.

¹²⁵ Le rapport au Roi précise en outre qu'« *Ils sont pour la plupart nés localement, dans la zone de conflit djihadiste, et n'existent donc pas officiellement. Leur enregistrement dans la banque de données commune T.E.R. constitue la seule manière d'avoir connaissance de leur existence vu qu'ils ne sont pas inscrits dans le Registre national* »

¹²⁶ « *Ces enfants pourraient ainsi éventuellement être abordés dans le CSIL-R, et les services socio-préventifs pourraient initier un accompagnement si nécessaire. Ces enfants sont effectivement considérés comme des personnes vulnérables, des victimes pour lesquels il est essentiel d'assurer un suivi spécifique au cas par cas. Ils ne sont pas discutés à la [TFL], à moins qu'une radicalisation problématique ne se produise au fil des ans* ».

¹²⁷ Ar. 6, §2, 1°, 1) du projet de loi

¹²⁸ Pour un exemple de cas où le fait de se retrouver sur une liste accroît les risques d'arrestation, voy. Saunders, J., Hunt, P. & Hollywood, J.S. Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot. *J Exp Criminol* 12, 347–371 (2016). <https://doi.org/10.1007/s11292-016-9272-0>

¹²⁹ Voir notamment : avis n° 129/2022 du 1^{er} juillet 2022 *concernant les articles 2 et 7 à 47 d'un projet de loi portant des dispositions diverses en matière d'Economie*, considérants nos 42 et s. ; avis n° 131/2022 du 1^{er} juillet 2022 *concernant un projet de loi portant création de la Commission du travail des arts et améliorant la protection sociale des travailleurs des arts*, considérants nos 55 et s. ; l'avis n° 112/2022 du 3 juin 2022 *concernant un projet de loi modifiant le Code pénal social en vue de la mise en place de la plateforme eDossier*, considérants nos 3-41 et 87-88 ; avis n° 231/2021 du 3 décembre 2021 *concernant un avant-projet d'ordonnance concernant l'interopérabilité des systèmes de télépéage routier*, considérants nos 35-37 ; l'avis n° 37/2022 du 16 février 2022 *concernant un avant-projet de décret instituant la plateforme informatisée centralisée d'échange de données 'E-Paysage'*, considérant n° 22 ; l'avis n° 13/2022 du 21 janvier 2022 *concernant un projet d'arrêté du*

108. Cela implique de préciser très clairement de quelle(s) autorité(s) relève la BDC (ou auprès de quelles autorités la BDC est instituée¹³⁰) et pourquoi. Une disposition adéquatement libellée à cet égard doit permettre de déterminer :

- si la BDC est « *commune* » aux services de base ou aux services de base ET aux services partenaires ou encore aux services participant (de droit ou sur invitation ?) aux TFL ;
- qui sont les préposés¹³¹ des responsables du traitement (s'agit-il de l'OCAM seul¹³², du responsable opérationnel (l'OCAM) et du gestionnaire de la BDC (la Police Fédérale)¹³³ et des services de base (mais quid du SGRS qui est l'un des « *services de renseignement et de sécurité* » visé par la loi du 30 novembre 1998, mais qui est placé sous l'autorité du Ministre de la Défense¹³⁴ ?) ;
- que les missions des services impliqués sont bien compatibles avec les finalités de la BDC ;
- si une modification des compétences de l'auteur de la norme est susceptible d'affecter les traitements de données à caractère personnel¹³⁵ ; et

Gouvernement de la Région de Bruxelles-Capitale relatif à l'octroi de primes à l'amélioration de l'habitat et un projet d'arrêté du Gouvernement de la Région de Bruxelles-Capitale modifiant l'arrêté du Gouvernement de la Région de Bruxelles-Capitale du 9 février 2012 relatif à l'octroi d'aides financières en matière d'énergie, considérants nos 9-17 ; l'avis n° 65/2019 du 27 février 2019 concernant un projet d'accord de coopération modifiant l'accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative, considérants nos 90-113.

¹³⁰ A cet égard le passage de « pour l'exercice conjoint des missions visées à l'article 44/2, § 2, les ministres de l'Intérieur et de la Justice peuvent conjointement créer des banques de données communes dont ils deviennent responsables du traitement » ([Art. 44/11/3bis](#), §1^{er}, LFP) à « il est créé une banque de données commune « *Terrorisme, Extrémisme, processus de Radicalisation* » qui permet le traitement commun, par tout ou partie des services de base et des services partenaires, des données à caractère personnel et des informations relatives aux missions de prévention et de suivi du terrorisme et de l'extrémisme, lorsqu'il peut mener au terrorisme (...) » pour laquelle l'OCAM est désignée responsable opérationnel (art. 3 du projet de loi et art. 5 du projet d'AR) est une régression problématique. Comp. : [Art. 8](#), §4, de la loi du 16 octobre 2022 visant la création du Registre central pour les décisions de l'ordre judiciaire et relative à la publication des jugements et modifiant la procédure d'assises relative à la récusation des jurés (MB 24.10.2022)

¹³¹ Par opposition aux « utilisateurs » qui doivent respecter les consignes d'accès et d'utilisation édictées par les responsables du traitements, mais qui ne sont pas placés sous leur autorité (en cas de traitement illicite, il sont donc susceptibles d'engager leur propre responsabilité, tant vis-à-vis des personnes concernées que vis-à-vis des responsables du traitement, mais PAS directement la responsabilité du responsable du traitement à l'égard des personnes concernées)

¹³² Qui est effectivement placé sous l'autorité conjointe des Ministres de l'Intérieur et de la Justice ([Art. 5](#) de la loi du 10 juillet 2006 relative à l'analyse de la menace (MB 20.07.2006))

¹³³ Qui sont tous deux placés sous l'autorité conjointe des Ministres de l'Intérieur et de la Justice (*Ibidem* et [Art. 5](#) LFP)

¹³⁴ [Art. 10](#), §2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (MB 18.02.1998)

¹³⁵ Concrètement, en cas (1) de création d'un nouveau service fédéré disposant de compétences de constatations et de poursuites d'infractions édictées par l'entité fédérée en question ou (2) de régionalisation (ou communautarisation) d'un service et de ses compétences, il s'agira de pouvoir déterminer si le facteur de rattachement du traitement (faits commis dans l'entité, auteur présumé domicilié dans l'entité, etc...) est compatible avec la compétence du législateur ayant déterminé les éléments essentiels du traitement. En effet, les données collectées et enregistrées durant la période durant laquelle le législateur fédéral était compétent sont susceptibles d'être traitées par une autorité régionale ou communautaire dans le second cas uniquement, mais seules les données disposant d'un lien de rattachement avec l'entité fédérée seront susceptibles d'être traitées ; A noter qu'habituellement, l'Autorité s'abstient de faire des observations relatives à une situation future dont rien n'indique qu'elle se produira. Cependant, au vu de l'importance de l'ingérence dans les droits et libertés des personnes concernées, l'Autorité estime que dès lors qu'il est possible de prendre en considération ce risque dès à présent, il ne pourrait être admis que la « *sécurité nationale* » soit valablement invoquée pour couvrir des traitements devenus illicites (au sens de l'art. 5.1.a) du RGPD) au motif que les normes régionales ou communautaires *ad hoc* (et/ou un accord de coopération) ne pourraient pas être adoptées avant la mise en œuvre effective d'une réforme de l'Etat.

- quel Titre de la LTD¹³⁶ est applicable au traitement des données à caractère personnel effectués sous la responsabilité des responsables du traitement de la BDC.

109. En ce qui concerne ce dernier alinéa, pour rappel, les normes applicables sont déterminées à la fois par l'autorité compétente concernée et par la finalité du traitement. Or, à défaut d'une disposition prévoyant « *la collecte des traitements par le responsable opérationnel auprès des services partenaires* »¹³⁷, il y a lieu de considérer que les services partenaires communiquent des données aux responsables du traitement de la BDC¹³⁸. Le RGPD s'applique donc pleinement à cette communication par les services partenaires¹³⁹ qui ne relèvent pas du champ d'application de la directive police-justice. L'art. 30, §2 du projet confirme cette interprétation. Le RGPD s'applique également à l'accès¹⁴⁰ par ces mêmes services partenaires, aux données de la BDC. Une fois ces données communiquées¹⁴¹, l'art. 30, §1^{er} prévoit que le responsable du traitement « *propre à chaque service* » qui alimente la BDC reste « *responsable de la qualité des données* », mais les responsables du traitement de la BDC sont responsables de la qualité des données à caractère personnel « *validées sur les fiches de renseignement* ». L'Autorité estime que cette formulation est problématique, car elle revient à exonérer les responsables du traitement de la BDC pour le traitement (par exemple la communication à des tiers) de données inexactes, alors que le respect du principe d'exactitude est une condition de licéité du traitement qui implique, le cas échéant, de s'abstenir de traiter (et surtout de communiquer) certaines données. Cet écueil provient du fait que l'exigence des normes relatives à la protection des données portent sur la désignation d'un responsable pour « *les traitements* » (et non uniquement de la banque de données)¹⁴². **Il y a donc lieu de déterminer, dans le projet, qui sont les responsables du traitement, en fonction des différents traitements susceptibles d'être réalisés et non en fonction de la banque de données.**

110. Ensuite, si la finalité des TFL est liée à l'alimentation de la BDC¹⁴³, dans un souci de prévisibilité, l'Autorité invite le demandeur à, détailler les raisons de l'absence d'alignement entre services de

¹³⁶ En d'autres termes, quels sont les traitements qui relèvent respectivement du RGPD, de la directive police-justice ou du Titre III et de la Convention 108 du Conseil de l'Europe

¹³⁷ Pour rappel le projet prévoit l'abandon de la notion de « collecte » au profit de celle d'« enregistrement » pour correspondre à la réalité IT

¹³⁸ Il sera toutefois prêté attention aux observations relatives au caractère adéquat de l'application de la notion de responsable du traitement à une banque de données, formulées dans le présent chapitre

¹³⁹ Tels que par exemple l'OE

¹⁴⁰ Qu'il s'agisse d'un accès en lecture ou par interrogation directe

¹⁴¹ C'est-à-dire après avoir « *alimenté* » la BDC

¹⁴² Bien entendu, la détermination d'un responsable du traitement pour une banque de données, n'est pas une mauvaise pratique en soi

¹⁴³ Sans préjudice des critiques formulées *supra* lors de l'analyse des finalités.

base/partenaires de la BDC et participants de droit ou invités aux coordinations dans le cadre des TFL¹⁴⁴, dans l'exposé des motifs.

111. En ce qui concerne la communication prévue à l'art. 28, l'Autorité estime qu'il y a lieu de préciser dans le commentaire, quelle est l'autorité visée par les obligations légales (ou les Traités) pour la communication des données figurant dans la BDC. S'il s'agit des différents services à l'origine de la collecte des données, chacun pour ses propres données, la possibilité de réaliser des transferts internationaux de données contenues dans la BDC pourrait être purement et simplement omise (ou, à défaut, devrait être dûment justifiée). Si par contre, c'est le responsable opérationnel qui est assujéti à cette obligation de communication, il y a lieu de s'assurer de la validité de l'engagement de l'OCAM en ce qui concerne la communication des données communiquées par les autres services¹⁴⁵ ou d'en conclure que la BDC est une banque de données OCAM accessible à d'autres services. Le projet sera donc revu en fonction de l'une ou l'autre hypothèse.

II.5. Durée de conservation des données traitées

112. En vertu de l'article 5.1.e) du RGPD, 28, 5° et 77 LTD, les données à caractère personnel ne peuvent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées.
113. La durée de conservation maximale des données est fixée à 60 ans « *après leur dernier traitement* » (art. 7 du projet de loi)¹⁴⁶.
114. Cette durée s'explique par la pratique de l'archivage (entre les mains du responsable du traitement et non par envoi aux Archives générales du Royaume) qui, en vertu de la même disposition, intervient au plus tard 30 ans « *après le dernier traitement* ».
115. L'Autorité estime tout d'abord que le critère du « *dernier traitement* » est susceptible de justifier une conservation infinie des données à caractère personnel concernées. L'Autorité recommande donc d'avoir égard à un critère objectif, tel que par exemple le dernier devoir d'enquête relatif à l'entité concernée.

¹⁴⁴ Visés aux art. 31 et sv. du projet de loi (sur cette question voy. *infra*)

¹⁴⁵ Par exemple, est-ce que l'OCAM est habilitée à communiquer des données obtenues des Affaires consulaires à des services étrangers qui ne sont pas les homologues des Affaires consulaires ?

¹⁴⁶ La durée d'archivage est cependant réduite pour les entités en pré-enquête (voy. *supra*) et il est prévu que l'archivage intervienne après 15 ans pour les mineurs

116. Ensuite, l'Autorité estime que, s'agissant de données détenues au moins partiellement par chacun des services faisant partie de la chaîne pénale et de sécurité, le caractère nécessaire et proportionné d'un archivage séparé, au niveau de la BDC, doit être démontré. En tout état de cause, l'Autorité estime qu'il convient de prévoir que ces données archivées ne devraient plus pouvoir être communiquées aux services autres que les membres des services relevant de la chaîne pénale et de sécurité (dans la mesure où l'art. 7, §2, 2° ne semble pas totalement l'exclure).

117. Par ailleurs, l'Autorité relève que la durée d'archivage est fixée sous forme de maximum. Il y a donc lieu d'assortir la possibilité d'effacement anticipé de conditions (comme cela a été prévu pour l'archivage)¹⁴⁷.

118. Compte tenu de l'importance des conséquences liées au traitement de ces données (et en particulier pour les personnes vulnérables qui ne pourront mettre en œuvre les voies de recours qu'au prix de très importantes difficultés), l'Autorité estime que la vérification des conditions de conservation dans la BDC ou dans les archives de la BDC doit intervenir à intervalle plus régulier¹⁴⁸. Sous réserve de la démonstration de la nécessité de retenir un autre délai, l'Autorité recommande une vérification annuelle et un archivage après 5 ans de vérifications infructueuses (ou en l'absence de vérification régulière durant les 5 dernières années). Des vérifications plus espacées pourraient en revanche être admissibles pour l'effacement.

Par ces motifs,

L'Autorité est d'avis que

- le sort des 47 services partenaires ayant accès à la BDC doit être clarifié (point 11) ;
- les délégations contenues aux articles 6, 9, 33 et 40 du projet de loi doivent être limitées aux modalités d'exécution des éléments essentiels devant figurer dans le projet de loi (point 21) ;
- l'habilitation au Roi contenue à l'art. 8 doit être omise et il y a lieu de prévoir que « *l'ensemble des traitements des données figurant dans la banque de données communes, en ce compris leur enregistrement, font l'objet d'une journalisation* » (point 22) ;
- « *l'extraction* » des listes (visée à l'art. 26, §1^{er}) par les services ayant un droit de lecture doit être couverte par une obligation de journalisation (point 23) ;

¹⁴⁷ A savoir, si les données à caractère personnel ne présentent plus un lien direct avec l'une des finalités de l'article 5, alinéa 2

¹⁴⁸ Le projet prévoit actuellement 5 ans (et 3 ans pour les mineurs)

- les normes organiques des services disposant d'un droit d'écriture doivent prévoir que la collecte des données susceptibles d'être enregistrées dans la BDC doit avoir été journalisée (point 24) ;
- le contrôle périodique des fichiers de journalisation doit être prévu dans le projet et dans les normes organiques des services partenaires pour les traitements « *locaux* » (point 25) ;
- les nécessités stratégiques, tactiques et opérationnelles doivent être distinguées les unes des autres et décrites précisément dans la loi ou un arrêté d'exécution (point 30) ;
- les finalités liées à la création d'une banque de données doivent être distinguées des finalités des différents traitements réalisés par chacun des services relativement à ces données (point 31) ;
- le commentaire de l'art. 6 doit contenir la démonstration, pour chacun des services disposant d'un droit d'écriture, que la finalité de chacun des traitements ultérieurs de ces données est compatible avec la finalité pour laquelle elles ont été collectées (point 32) ;
- l'art 6 et son commentaire (de même que, le cas échéant, les normes organique des services partenaires) doivent être adaptés du point de vue de la finalité des traitement et du caractère nécessaire et proportionné de ceux-ci (points 35 et 36) ;
- les finalités des accès par les services partenaires doivent être déterminées pour chaque catégorie de donnée (point 37) ;
- la fixation de limites ou l'énonciation, dans l'exposé des motifs, de circonstances dans lesquelles un traitement serait constitutif d'un détournement de finalité est souhaitable (point 39) ;
- l'art 9 du projet doit mentionner que l'interconnexion de la BDC avec des sources authentiques en peut en aucun cas permettre à des autorités ne disposant pas d'un accès légal à ces sources, de se voir accéder aux données contenues dans ces sources authentiques (point 40) ;
- l'art. 31 du projet de loi doit être reformulé en veillant à l'aligner sur son commentaire (point 44) ;
- les finalités de la communication de données aux services invités à participer aux TFL doivent être précisées (point 46) ;
- il convient de déterminer si les TFL sont des plateformes de concertation organisées en application de l'art. 458^{ter} CP auquel cas l'Autorité souhaite que le projet adapté lui soit à nouveau soumis pour avis avant son adoption (point 47) ;
- si le demandeur souhaite créer une nouvelle exception légale au secret professionnel il y a lieu de reformuler le commentaire de l'art. 19 et de modifier le Code pénal en vue d'y introduire cette nouvelle typologie d'exception (point 49) ;

- le cas échéant, il convient de déterminer ce que le destinataire de l'information couverte par le secret professionnel a la possibilité et/ou l'obligation de faire avec les données communiquées (point 50) ;
- si l'intention du demandeur est d'appliquer cette disposition à d'autres intervenants et/ou autorités, il conviendra de préciser, dans le commentaire de l'article 19, lesquelles et de quelle manière (point 52) ;
- le cas échéant, il convient de préciser les données des participants à une concertation en CSIL sont susceptibles d'être traitées à des fins répressives (point 53) ;
- qu'il y a lieu d'intégrer une référence aux travaux préparatoires de la loi de 2014 dans le commentaire de l'art. 7 et, concernant la finalité du traitement des données archivées, d'en démontrer le caractère légitime (point 57) ;
- le libellé de la finalité du traitement ultérieur visée aux art. 4, 24, 28 et 46 doit permettre de déterminer leur compatibilité avec la finalité pour laquelle les données ont été initialement collectées (point 58) ;
- il convient de mentionner (à l'art. 4 du projet) que des statistiques seront réalisées aux fins de la publication d'un rapport d'évaluation portant sur l'efficacité des moyens de traitements mis en œuvre et des autorités impliquées par la loi en projet et son arrêté d'exécution par rapport aux finalités pour lesquelles les données ont été enregistrées dans la BDC (points 59, 78, 81 et 97) ;
- l'impact du projet sur le fonctionnement des CSIL-R doit être clarifié (points 61 à 63) ;
- la possibilité de communication d'une carte d'information à une autorité ou une institution tierce doit être reformulée (points 65 et 66) ;
- le fondement légal et les limites de la délégation de la précision des finalités de communication aux bourgmestres, au Roi doivent être mentionnés (point 67) ;
- l'art 12 du projet d'AR doit être aligné sur le rapport au Roi (point 69) ;
- la qualité en vertu de laquelle un bourgmestre est susceptible d'être destinataire de données à caractère personnel doit être déterminée (points 70 et 71) ;
- en ce qui concerne la compétence du bourgmestre définie dans la nouvelle loi communale, il y a lieu de se référer aux « *mesures de police administratives* » (point 72) ;
- le cas échéant, le projet doit être adapté afin de préciser les finalités du traitement au regard des compétences légales du bourgmestre en matière de concertations de cas au sens de l'art. 458 CP (point 73) ;
- l'exposé des motifs du projet doit contenir une justification du caractère nécessaire et proportionné de la participation de chacun des nouveaux partenaires ainsi que du maintien de chacun des services participant actuellement par rapport à la possibilité d'atteindre la finalité visée par une communication de certaines données par l'un des services de base seul (points 79 et 80) ;

- la démonstration du caractère nécessaire et proportionné de la communication devra également porter sur les modalités de cette communication (point 82) ;
- le besoin de communication des données avec d'autres partenaires que la VSSE, l'OCAM et la Police Fédérale n'est ni exprimé, ni démontré (point 87) ;
- le caractère nécessaire et proportionné de la participation de l'OE aux TFL n'est pas démontrée dans l'état actuel du projet et ne semble pas démontrable à l'aide du cas cité en commentaire (point 89) ;
- la concertation préalable obligatoire doit être distinguée de la communication en temps réel ou a posteriori de l'information relative à la prise d'une mesure, avec les services disposant de données à l'égard de l'intéressé (point 90) ;
- les services susceptibles d'être invités doivent à tout le moins être déterminables (point 91) ;
- la notion d' « échange » de données doit être précisée (point 92) ;
- il y a lieu de reformuler l'art. 6 du projet de loi en distinguant – pour chacun des services partenaires - les catégories de données dont ces services disposent et sont habilités à communiquer en vertu de ce projet « *dans le respect du besoin d'en connaître* » des autres services, des données communiquées par d'autres participants, en réunion de concertation, dont les autres services participants ont la possibilité de prendre connaissance (point 95) ;
- à chaque fois que la finalité pourra être atteinte par la communication de données d'un seul service (par exemple un extrait de l'analyse de la menace de l'OCAM ou un rapport de la police locale), il soit procédé de la sorte (point 96) ;
- il convient de prévoir que les données contenues dans des banques de données policières ne pourront être traitées, par les services partenaires, que pour autant que leur caractère exact ait pu être établi par le biais d'un « *flux retour justice* » (point 98) ;
- il convient de prévoir que les condamnations mineures, figurant dans le casier judiciaire, étrangères aux infractions terroristes visées au titre *Iter* du Livre II du Code pénal, voire très anciennes ne doivent pas être traitées par les services partenaires (point 99) ;
- l'art. 44/1, §3, 2° LFP doit être reproduit dans le projet (point 100) ;
- le caractère nécessaire et proportionné du traitement des données relatives aux opinions politiques et aux convictions religieuses ou philosophiques, par chacun des services susceptibles d'en prendre connaissance, devra également être démontré dans le commentaire de l'art. 6 (point 101) ;
- une description des mesures techniques et organisationnelles, visant à garantir que des données communiquées par le service compétent dans le cadre d'une finalité liée à la prévention du terrorisme, ne puissent pas être traitées à d'autres fins par d'autres autorités, doit figurer dans le projet (point 102) ;

- il y a lieu de préciser dans le commentaire des art. 24 qu'il ne s'agit pas de permettre aux « *autres destinataires* » de la carte d'information de se prévaloir de cette disposition pour « *enquêter* », ni de consolider les données dont ils disposent au sujet des « *entités* », grâce à des informations qui seraient irrelevantes pour leurs propres finalités (point 103) ;
- le caractère nécessaire et proportionné du traitement des données à caractère personnel des entités, doit être démontré service par service (point 104) ;
- le traitement des données à caractère personnel des enfants mineurs de certaines entités outrepassé les finalités de l'enregistrement dans une banque de données accessible à des services dont les missions sont autres que celles des services de renseignement (point 105) ;
- il convient de préciser très clairement dans le projet de loi de quelle(s) autorité(s) relève la BDC (ou auprès de quelles autorités la BDC est instituée) et pourquoi (point 108) ;
- il y a lieu de déterminer, dans le projet, qui sont les responsables du traitement, en fonction des différents traitements susceptibles d'être réalisés et non en fonction de la banque de données (point 109) ;
- les raisons de l'absence d'alignement entre services de base/partenaires de la BDC et participants de droit ou invités aux coordinations dans le cadre des TFL doivent être détaillées dans l'exposé des motifs (point 110) ;
- il y a lieu de préciser dans le commentaire de l'art. 28, quelle est l'autorité visée par les obligations légales (ou les Traités) pour la communication des données figurant dans la BDC (point 111) ;
- le critère du « *dernier traitement* » pour la détermination du délai maximal d'archivage doit être abandonné (point 115) ;
- le caractère nécessaire et proportionné d'un archivage séparé, au niveau de la BDC, doit être démontré (point 116) ;
- les données archivées ne devraient plus pouvoir être communiquées aux services autres que les membres des services relevant de la chaîne pénale et de sécurité (point 116) ;
- il y a lieu d'assortir la possibilité d'effacement anticipé de conditions (point 117) ;
- la vérification des conditions de conservation dans la BDC ou dans les archives de la BDC doit intervenir à intervalle plus régulier (point 118).



Pour le Centre de Connaissances,
Cédrine Morlière - Directrice



ANNEXE

Principales abréviations:

BDC	Banque de données commune
BELPIU	Unité belge de l'Information des passagers
C.O.C	Organe de contrôle de l'information policière
CPPL	Commission permanente de la police locale
Comité R	Comité permanent de contrôle des services de renseignements
CSIL-R	Cellule de Sécurité Intégrale Locale en matière de radicalisme, d'extrémisme et de terrorisme
EPV	Extrémistes potentiellement violents
ETIAS	European Travel Information and Authorisation System
FTF	Foreign terrorist fighters
GPI	Police intégrée
HTF	Homegrown terrorist fighters
LFP	Loi sur la fonction de police
OCAM	Organe de Coordination pour l'Analyse de la Menace
O.E.	Office des Etrangers
PH	Propagandistes de haine
SGRS	Service Général du Renseignement et de Sécurité
T.E.R.	Terrorisme, extrémisme et radicalisme
TFL	Task Forces Locales
VSSE	Sûreté de l'Etat



Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 97/2023 van 16 juni 2023

Betreft: Adviesaanvraag met betrekking tot

- 1) een voorontwerp van wet tot oprichting van de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" ("T.E.R.") en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt (CO-A-2023-144) en**
- 2) Ontwerp van koninklijk besluit betreffende de gemeenschappelijke gegevensban T.E.R. (CO-A-2023-145)**

Vertaling¹

Het Kenniscentrum van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit"),
aanwezig: de dames Cédrine Morlière, Nathalie Raghenon en Griet Verhenneman, en de heren Yves-Alexandre de Montjoye en Bart Preneel;

Gelet op de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, met name de artikelen 23 en 26 (hierna "WOG");

Gelet op artikel 25, lid 3, van de WOG, volgens hetwelk de beslissingen van het Kenniscentrum bij meerderheid van stemmen worden aangenomen;

Gelet op Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (hierna "AVG");

¹ Voor de oorspronkelijke versie van de tekst, die collegiaal werd gevalideerd, cf. de Franse versie van de tekst, die beschikbaar is in de FR-versie van de rubriek "adviezen" van de website van de Autoriteit.

Gelet op de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (hierna "WVG");

Gelet op het verzoek om advies van de heer Vincent Van Quickenborne, Vice-eersteminister en Minister van Justitie en Noordzee, (hierna: de aanvrager) ontvangen op 13.04.2023;

Brengt op 16 juni 2023 het volgende advies uit² :

I. Onderwerp en context van de adviesaanvraag

1. De aanvrager heeft de Autoriteit om advies gevraagd over een voorontwerp van wet tot oprichting van de gemeenschappelijke gegevensbank T.E.R. (hierna "de GGB") en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt (hierna "wetsontwerp") evenals een ontwerp van Koninklijk Besluit met betrekking tot de GGB (hierna "ontwerp KB").
2. Er moet worden opgemerkt dat alleen de nieuwigheden worden toegelicht en becommentarieerd in de memorie van toelichting. Wat de bestaande bepalingen betreft die zonder inhoudelijke wijziging zijn overgedragen, wordt verwezen naar de motiveringen die aan de aanneming ervan ten grondslag liggen en die zijn opgenomen in de voorbereidende werkzaamheden voor de wet van 27 april 2016 houdende aanvullende maatregelen ter bestrijding van het terrorisme³ en in de verslagen aan de Koning van de hierboven vermelde uitvoerende KB's.
3. Toen hij zijn adviesaanvraag indiende, preciseerde de afgevaardigde ambtenaar dat het advies van de GBA uitsluitend werd gevraagd over de deelname van diensten «aan de werking van de GGB», die niet onder de bevoegdheid van het COC en het Comité I vallen. Bijgevolg moet, zelfs wanneer dit niet uitdrukkelijk in dit advies wordt vermeld, alleen rekening worden gehouden met de opmerkingen van de Autoriteit «voor zover de verwerking van persoonsgegevens waarin een gewijzigde versie van deze ontwerpen voorziet, nog andere diensten omvat dan de diensten die onder de bevoegdheid van het COC en het Comité I vallen».

a) Aangaande de GGB

² Een lijst met de belangrijkste afkortingen is als bijlage bij dit advies gevoegd.

³ Doc. 54-1727/001 en volgende.

4. Het wetsontwerp beoogt de bepalingen van de wet op het politieambt (hierna "WPA") met betrekking tot de GGB's⁴ om te zetten in een specifieke wet en er, om het met de woorden uit de memorie van toelichting te zeggen, «zoveel mogelijk elementen» die *tot nu toe* in de uitvoeringsbesluiten waren opgenomen, in op te nemen.
5. Artikel 3 van het wetsontwerp bepaalt dat de GGB «*de gemeenschappelijke verwerking mogelijk maakt, door alle of een deel van de basisdiensten⁵ en de partnerdienst⁶, van de persoonsgegevens en informatie betreffende de opdrachten inzake de voorkoming en de opvolging van terrorisme en extremisme, dat kan leiden tot terrorisme(...) ⁷, , elk in het kader van zijn wettelijke bevoegdheden* ».
6. In vergelijking met de huidige situatie beogen de ontwerpen (1) de toegangsrechten te schrappen die tot nu toe genoten werden door de Nationale Veiligheidsoverheid en het Vast Comité van de Lokale Politie (hierna "la VCLP"), (2) de toegangsrechten van de dienst Erediensten en Vrijzinnigheid en de Administratie van de Thesaurie - tot nu toe vastgelegd in een KB - te vermelden (en de facto uit te breiden) in de wet, (3) de toegangsrechten van de dienst Douane en Accijnzen en het Crisiscentrum uit te breiden (maar, wat deze laatste betreft, enkel voor de gedetacheerden van de politie en de Staatsveiligheid (hierna "la VSSE") binnen de BELPIU⁸ en de ETIAS-eenheid⁹) en (4) nieuwe toegangsrechten te creëren ten voordele van de dienst voor de hulpverlening aan de jeugd van de Franse Gemeenschap en de dienst voor de hulpverlening aan de jeugd van de Duitstalige Gemeenschap.
7. Enkel de basisdiensten zullen (op eigen initiatief of op voorstel van een partnerdienst) een "*entiteit creëren*" of een inlichtingenfiche¹⁰ waarover, na validatie door OCAD, alle basisdiensten en

⁴ Opgericht door het Koninklijk Besluit van 21 juli 2016 met betrekking tot de GGB "Terrorist Fighters" en door het Koninklijk Besluit van 23 april 2018 met betrekking tot de GGB "Haatpropagandisten".

⁵ Namelijk OCAD, de geïntegreerde politie (hierna "GP") en de inlichtingen- en veiligheidsdiensten (art. 2, 2°). Het commentaar bij dit artikel preciseert «*het gaat om politie- of analysediensten die bij hun werk rechtstreeks in eerste lijn met de T.E.R.-entiteiten en -doeleinden te maken hebben of waarvan het analyserend werk op die entiteiten betrekking heeft en die bijgevolg het grootste aandeel gegevens met betrekking tot die entiteiten ter beschikking kunnen hebben of als allereerste een nieuwe T.E.R.-entiteit kunnen opsporen*».

⁶ Namelijk de "operationele eenheden" van het Nationaal Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken; de Algemene Directie Veiligheid en Preventie van de Federale Overheidsdienst Binnenlandse Zaken; het Directoraat-generaal Penitentiaire Inrichtingen van de Federale Overheidsdienst Justitie; het Directoraat-generaal Consulaire Zaken van de Federale Overheidsdienst Buitenlandse Zaken; het Openbaar Ministerie; de Cel voor Financiële Informatieverwerking, de Algemene Administratie van de douane en accijnzen van de Federale Overheidsdienst Financiën, de dienst Erediensten en Vrijzinnigheid van de Federale Overheidsdienst Justitie, de Algemene administratie van de Thesaurie van de Federale Overheidsdienst Financiën, de Algemene Administratie van Justitiehuisen van de Franse Gemeenschap, het departement Justitiehuis van het Ministerie van de Duitstalige gemeenschap, het Vlaams Agentschap Justitie en Handhaving, de Algemene Administratie van de hulpverlening aan de jeugd van de Franse Gemeenschap, de dienst voor de hulpverlening aan de jeugd van de Duitstalige gemeenschap en het Vlaams Agentschap Opgroeien.

⁷ Als bedoeld in artikel 8, 1°, b) en c) van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst

⁸ de Passagiersinformatie-eenheid bedoeld in hoofdstuk 7 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens.

⁹ Ook genoemd BelENU, opgericht bij Verordening EU 2018/1240.

¹⁰ Vooral met betrekking tot een fysiek persoon.

partnerdiensten met schrijfrechten¹¹ zullen communiceren en de (niet-geklasseerde) gegevens die ze bezitten zullen registreren. Er wordt uitdrukkelijk bepaald dat deze inlichtingenfiches mogen worden meegedeeld aan bestemmingen die "geen partner" zijn (bv. de burgemeester)¹².

8. Gegevens over iemands gezondheid (lichamelijk en geestelijk) en gegevens over gevaarlijkheid die in de GGB zijn opgenomen, kunnen door de basisdiensten ook worden doorgegeven aan gezondheidszorgverleners¹³.
9. Het ontwerp voorziet ook in de mogelijkheid om andere "operationele" gegevensbanken van een basisdienst of partnerdienst of met een authentieke bron (bv. het Rijksregister of de DIV) te koppelen, zodat de GGB automatisch kan worden gevoed met gegevens uit authentieke bronnen of hits kan detecteren door GGB-gegevens automatisch te vergelijken met de operationele gegevensbanken van basisdiensten en partnerdiensten¹⁴.
10. Artikel 3 van het wetsontwerp vermeldt de oprichting van « *een* » GGB. In dit verband merkt de Autoriteit op dat de verwijzing in de wet naar de unieke aard van de GGB nieuw is in vergelijking met de formulering van de teksten die het moet vervangen¹⁵ en met de interpretatie van het COC, het Comité I¹⁶ en de Raad van State¹⁷. De Autoriteit gaat ervan uit dat dit de verwezenlijking is van de «(de samenvoeging die) aan de orde is» die is aangekondigd in het Verslag aan de Koning bij het

¹¹ Krachtens het ontwerp van koninklijk besluit zijn van de 11 partnerdiensten die in artikel 2 van het wetsontwerp worden opgesomd, alleen de DG's Veiligheid en Preventie, Consulaire Zaken en de Dienst Erediensten en Vrijzinnigheid beperkt tot een zoekopdracht (hit/no hit) van de GGB. Alle andere hebben een schrijfrecht.

¹² Art. 24 van het wetsontwerp

¹³ Art. 6, § 2 van het wetsontwerp

¹⁴ Art. 9 van het wetsontwerp; Voor een voorbeeld van de implementatie van technieken, zoals *private set intersection* die toelaten voor organisatie A om na te gaan welke mensen in hun lijst voorkomt in een database van organisatie B, zie Roel Peeters, Andreas Pashalidis : Privacy-Friendly Checking of Remote Token Blacklists. IDMAN 2013, Policies and Research in Identity Management - Third IFIP WG 11.6 Working Conference, IDMAN 2013, London, UK, April 8-9, 2013. Proceedings blz. 18-33. <https://www.esat.kuleuven.be/cosic/publications/article-2303.pdf>

¹⁵ Onderafdeling 7bis van de WPA, waarin de bepalingen met betrekking tot de GGB zijn opgenomen, is getiteld "Gemeenschappelijke gegevensbanken" en de koninklijke besluiten verwijzen enerzijds naar "de gemeenschappelijke gegevensbank van Terrorist Fighters" (hierna "GGB FTF") (koninklijk besluit van 21 juli 2016) en anderzijds naar "de gemeenschappelijke gegevensbank van Haatpropagandisten" (hierna "GGB HP") (koninklijk besluit van 23 april 2018) ; Zie ook het verslag aan de Koning bij het Ontwerp KB GGB HP dat het volgende stelde «*Hoewel de specifieke doeleinden van de gemeenschappelijke gegevensbank Haatpropagandisten, en de gegevens en informatie die erin vervat zitten, verschillen van deze van de gemeenschappelijke gegevensbank Terrorist Fighters, heeft de gemeenschappelijke gegevensbank Haatpropagandisten dezelfde hoofddoelstelling voor ogen, met name de strijd tegen het terrorisme [...]*».

¹⁶ In de Memorie van Toelichting bij het wetsontwerp wordt verduidelijkt: «*in tegenstelling tot wat het Controleorgaan op de Politie Informatie (COC) en het Vast Comité I in hun verslag van 2020 aangeven, staat de gemeenschappelijke gegevensbank 'Haatpropagandisten' niet los van de gemeenschappelijke gegevensbank 'Terrorist Fighters'*»; Deze behoefte aan verduidelijking is des te bedenkelijker omdat, volgens artikel 44/11/3bis, §3 van WPA, de verwerkingsverantwoordelijken de oprichting van een GGB moeten melden bij het COC en het Comité I.

¹⁷ Naar aanleiding van advies nr. 62.629/2 - 62.630/2, uitgebracht op 31 januari 2018 over twee ontwerpen van koninklijk besluit, het ene tot wijziging van het koninklijk besluit GGB FTF en het andere met betrekking tot het GGB HP, stelde de afdeling Wetgeving van de Raad van State dat " «*il y a lieu d'examiner le choix de l'auteur du texte de multiplier les banques de données liées à la lutte contre le terrorisme et l'extrémisme pouvant mener au terrorisme puisqu'à côté de la banque de données commune Terrorist Fighters « T.F. » (projet n° 62.629/2) est envisagée la création d'une nouvelle banque de données commune qui concerne les « Propagandistes de haine » (projet n° 62.630/2) »* » (<http://www.raadvst-consetat.be/dbx/avis/62629.pdf>, p. 15)

ontwerp van Koninklijk Besluit van 20 december 2019¹⁸. In ieder geval is dit (net als de opsomming in de wet van alle diensten met toegang tot de GGB¹⁹) geen triviale verandering, aangezien bijvoorbeeld de Dienst Erediensten en Vrijzinnigheid, die tot nu toe alleen wettelijke toegang had tot de GGB HP²⁰ (krachtens het Koninklijk Besluit van 23 april 2018)²¹, nu een wettelijke basis zal hebben voor toegang tot "het geheel" van de GGB.

11. Bij het lezen van deze wijzigingen en het aantal "gecentraliseerde" diensten in het ontwerp met toegang tot de GGB, blijft er twijfel bestaan over het lot dat de aanvrager wil reserveren voor alle "47 partnerdiensten" » "met toegang tot de GGB waarnaar wordt verwezen in het activiteitenverslag 2019 van Comité I²². De Autoriteit is van mening dat dit punt moet worden verduidelijkt.
12. De Autoriteit wijst erop dat zij en haar rechtsvoorganger - de Commissie voor de bescherming van de persoonlijke levenssfeer - tal van adviezen hebben uitgebracht over ontwerpen voor wet- en regelgeving in verband met de GGB²³. Aangezien de bevoegdheid van de Autoriteit momenteel²⁴ wordt

¹⁸ «(...) moeten we vaststellen dat de Raad van State gelijk heeft wanneer zij enerzijds stelt dat een rechtvaardiging ontbreekt wat betreft de noodzaak om twee verschillende koninklijke besluiten te hebben voor de Terrorist Fighters en de Haatpropagandisten en anderzijds wanneer zij aanhaalt dat het moeilijk is om te bepalen of de gegevens over de P.G.E. en Terrorisme veroordeelden verwerkt moeten worden in het koninklijk besluit over de Terrorist Fighters of de Haatpropagandisten. In principe gaat het om één enkele gegevensbank die ingedeeld is in verschillende categorieën van personen die in de gegevensbank verwerkt kunnen worden. Echter, gezien enerzijds de dringende noodzaak om over een wettelijke basis te kunnen beschikken om de gegevens te verwerken van P.G.E. en Terrorisme veroordeelden en anderzijds de periode van lopende zaken, hebben de opstellers beslist om deze twee nieuwe categorieën in het koninklijk besluit betreffende de Terrorist Fighters te integreren. Dit koninklijk besluit herneemt immers de meeste categorieën van personen van wie gegevens verwerkt worden in het kader van de gemeenschappelijke gegevensbanken. Op termijn is een samenvoeging van het koninklijk besluit Terrorist Fighters en het koninklijk besluit Haatpropagandisten dus aan de orde» (Verslag aan de Koning - Koninklijk besluit tot wijziging van het Koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Terrorist Fighters en van het koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten, <http://www.eiustice.iust.fgov.be/wet/wet.htm>).

¹⁹ Waarover in de Memorie van Toelichting wordt verduidelijkt dat dit gebeurt «met het oog op centralisering en leesbaarheid» »

²⁰ En niet de gegevens die de GGB (F)TF zou moeten bevatten

²¹ In een verslag van de Comités I en P over de ondersteunende diensten van OCAD staat in dit verband : «in de loop van het gesprek van 10 juli 2020 heeft de dienst Erediensten en Vrijzinnigheid er ons op gewezen dat hij volledige toegang had tot de GGB en dus de mogelijkheid had om die databank te voeden. Niettemin is gebleken dat er geen wettelijke basis is om hen die volledige toegang toe te kennen (ze hebben wettelijk gezien enkel toegang tot de GGB HP door rechtstreekse bevraging). Deze volledige toegang is volgens hen nochtans noodzakelijk opdat ze rechtstreeks de GGB zouden kunnen raadplegen in het kader van hun bevoegdheden. Ze schuiven voornamelijk twee argumenten naar voren om deze keuze voor een volledige toegang te verklaren: - de dienst Erediensten en Vrijzinnigheid moet de mogelijkheid hebben om de GGB te voeden indien dat relevant blijkt te zijn (bv. rechtspersonen die nog niet opgenomen zijn in de GGB maar die dat zouden kunnen zijn) - de opzoeken die maandelijks worden verricht, zijn niet mogelijk met een "HIT, NO HIT"-systeem. Begin november 2020 heeft de dienst Erediensten en Vrijzinnigheid verduidelijkt dat ze met het OCAD aan het werken waren om hun volledige toegang tot de GGB te regulariseren. In afwachting werd beslist om hun toegang tot de GGB te beperken tot een HIT - NO HIT. Ze hebben in dit stadium dus nog altijd toegang tot het geheel van entiteiten van de GGB want de federale politie, technisch beheerder van de GGB, kan deze toegang op technisch vlak niet opdelen. (Enquête de contrôle sur les services d'appui de l'OCAM l'AR du 17 août 2018, note 51, p. 24

<https://www.comiteri.be/images/pdf/enquetes/2%20NL%20TO%202020%20278%20Nieuwe%20Ondersteunende%20diensten%20OCAD%20NL.pdf>

²² http://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag%2019_FR.pdf, p. 89 (zie eveneens blz. 89 en 89).

²³ Adviezen nr. 57/2015 van 16 december 2015, nr. 31/2016 van 29 juni 2016, nr. 4/2018 van 17 januari 2018 en nr. 5/2018 van 17 januari 2018.

²⁴ Sinds de inwerkingtreding van de wet van 22 mei 2019 tot wijziging van diverse bepalingen wat het politieke informatiebeheer betreft (MB 19.06.2019).

beperkt door de bevoegdheid van het COC en het Comité I, verwijst de Autoriteit naar hen voor aspecten die niet in dit advies worden behandeld.

b) Aangaande de Lokale Task Forces

13. Er wordt ook bepaald dat de persoonsgegevens van de betrokkenen (die onder het hierboven vermelde begrip " entiteit " vallen) moeten worden geraadpleegd door de basisdiensten en de partnerdiensten met het oog op (1) gecoördineerd overleg tussen de basisdiensten en de partnerdiensten, (2) de strategische, tactische of operationele noodzaak om persoonsgegevens en informatie gezamenlijk te verwerken met het oog op de uitvoering van de respectieve taken van de basisdiensten en de partnerdiensten, (3) ondersteuning van besluitvorming door administratieve overheden of van besluitvorming door de bestuurlijke of gerechtelijke politie en (4) analyse, dreigingsevaluatie en toezicht, met inbegrip van het nemen van maatregelen, op in de GGB geregistreerde entiteiten en analyse, evaluatie en toezicht op het verschijnsel terrorisme en extremisme wanneer dit op basis van een dreigingsevaluatie tot terrorisme kan leiden.
14. Met dit in gedachten stelt de memorie van toelichting «*doel is ook om in het kader van de T.E.R.-strategie²⁵ de klemtoon te leggen op het noodzakelijke overleg tussen veiligheidsprofessionals over de gegevens in de gemeenschappelijke gegevensbank T.E.R., die het met elkaar eens moeten zijn over de wenselijkheid van het nemen van maatregelen wanneer een entiteit in de gemeenschappelijke gegevensbank wordt geregistreerd*». Het wetsontwerp beoogt deze doelstelling te bereiken door middel van de bepalingen van hoofdstuk 3 dat gewijd is aan overleg binnen lokale taskforces (hierna "LTF").

II. Onderzoek

II.1. Beginnelsen van transparantie en rechtmatigheid

15. Overeenkomstig artikel 6, lid 3, van de AVG²⁶, gelezen in het licht van overweging 41 van de AVG moet de verwerking van persoonsgegevens, die noodzakelijk is om te voldoen aan een

²⁵ Deze strategie, die op 8 september 2021 door OCAD werd aangekondigd, is een update van het Actieplan Radicalisme (R – Plan gepubliceerd in 2005 en voor het eerst bijgewerkt in 2015) en de omvorming ervan tot een strategische nota over extremisme en terrorisme (<https://ocad.belgium.be/wp-content/uploads/2021/09/Strategische-Nota-Extremisme-en-Terrorisme.pdf>)

²⁶ "41. Wanneer in deze verordening naar een rechtsgrond of een wetgevingsmaatregel wordt verwezen, vereist dit niet noodzakelijkerwijs dat een door een parlement vastgestelde wetgevingshandeling nodig is, onverminderd de vereisten overeenkomstig de grondwettelijke orde van de lidstaat in kwestie. Deze rechtsgrond of wetgevingsmaatregel moet evenwel duidelijk en nauwkeurig zijn, en de toepassing daarvan moet voorspelbaar zijn voor degenen op wie deze van toepassing is, zoals vereist door de rechtspraak van het Hof van Justitie van de Europese Unie („Hof van Justitie”) en het Europees Hof voor de Rechten van de Mens”.

wettelijke verplichting²⁷ en/of voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag²⁸ dat aan de verwerkingsverantwoordelijke is opgedragen, worden geregeld door duidelijke en nauwkeurige regelgeving, waarvan de toepassing voor de betrokkenen voorspelbaar moet zijn. Bovendien is het volgens artikel 22 van de *Grondwet* noodzakelijk dat de "wezenlijke elementen" van de gegevensverwerking door middel van een formele wettelijke norm worden vastgesteld.

Inmenging

16. De Autoriteit benadrukt van meet af aan dat het ontwerp **een aanzienlijke inmenging vormt op de rechten en vrijheden van de betrokken personen**, en wel om de volgende redenen.

- de verwerking heeft betrekking op "*gevoelige gegevens*" in de zin van artikel 9 en 10 van de AVG;
- de verwerking van persoonsgegevens gebeurt voor controle - en/of bewakingsdoeleinden;
- de verwerking van persoonsgegevens omvat het kruisen of combineren van verschillende informatie over de betrokkene uit twee (of meer) gegevensverwerkingen die oorspronkelijk voor verschillende doeleinden en/of door verschillende verwerkingsverantwoordelijken zijn uitgevoerd op zodanige wijze dat het de redelijke verwachtingen van de betrokkene overstijgt;
- de verwerking van persoonsgegevens heeft waarschijnlijk betrekking op kwetsbare personen²⁹ (in het bijzonder minderjarigen, vluchtelingen, asielzoekers of migranten, personen met psychische stoornissen, ...) ; en
- de verwerking van persoonsgegevens maakt het moeilijker voor betrokkenen om hun rechten uit te oefenen.

17. De Autoriteit wijst er ook op dat de deelname van nieuwe actoren tot gevolg heeft (en zelfs tot doel heeft) dat er meer persoonsgegevens worden verwerkt en dat deze gegevens kunnen worden gecombineerd, waardoor de rechten en vrijheden van de betrokken personen meer worden aangetast.

²⁷ Art. 6.1.c) van de AVG.

²⁸ Artikel 6.1.e), van de AVG.

²⁹ Er is sprake van kwetsbare personen wanneer er een bestaan is van « (...) *déséquilibre des pouvoirs accru qui existe entre les personnes concernées et le responsable du traitement, ce qui signifie que les premières peuvent se trouver dans l'incapacité de consentir, ou de s'opposer aisément au traitement de leurs données ou d'exercer leurs droits* » (S. Wattier et M. Nihoul, « Chapitre 1 - La protection de la personne en situation de vulnérabilité par le droit des libertés publiques dans l'environnement numérique » in H. Jacquemin et M. Nihoul (dir.), *Vulnérabilités et droits dans l'environnement numérique*, Bruxelles, Larcier, 2018, blz. 14 ev.).

18. Bijgevolg moeten overeenkomstig artikel 22 van de Grondwet de "essentiële elementen" van de verwerkingen met betrekking tot de in de GGB opgeslagen gegevens EN de tijdens het LTF-overleg meegedeelde gegevens in een norm van wetgevende rang worden omschreven. Het gaat om deze elementen: (het)(de) precieze en concrete doeleinde(n)³⁰, waarvan bij lezing reeds kan worden afgeleid welke gegevensverwerkingen zullen worden uitgevoerd voor de verwezenlijking ervan, de identiteit van de verwerkingsverantwoordelijke(n), de (categorieën van) gegevens die noodzakelijk zijn voor de verwezenlijking van (dit) (deze) doeleinde(n), de bewaartermijn van de gegevens³¹, de (categorieën van) betrokkenen van wie de gegevens zullen worden verwerkt, de (categorieën van) ontvangers aan wie de gegevens worden meegedeeld³², de omstandigheden waarin ze zullen worden meegedeeld, evenals de eventuele beperking van de verplichtingen en/of rechten vermeld in de artikelen 5, 12 tot en met 22 en 34 van de AVG.

Delegatie aan de Koning

19. Artikel 22 van de Grondwet verbiedt de wetgever om af te zien van de mogelijkheid om zelf te bepalen welke inmengingen het recht op eerbiediging van de persoonlijke levenssfeer kunnen beknotten³³. In deze context is een delegatie aan de Koning «*niet in strijd met het legaliteitsbeginsel voor zover deze delegatie voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de essentiële elementen voorafgaandelijk door de wetgever zijn vastgelegd*»³⁴.

20. In het onderhavige geval verleent het wetsontwerp de Koning onder meer de bevoegdheid om de categorieën van entiteiten (d.w.z. in het bijzonder de categorieën van betrokkenen) te bepalen van wie de gegevens worden verwerkt (art. 6), de doeleinden van de onderlinge koppeling (d.w.z. de

³⁰ Zie ook artikel 6.3 van de AVG.

³¹ Het Grondwettelijk Hof heeft reeds erkend dat " (...) vermocht hij (de wetgever) de vereisten inzake de bewaring van persoonsgegevens en de duur van die bewaring op een algemene wijze te regelen; Arrest nr. 29/2018 van 15 maart 2018, punt B.23.

³² Zie bijvoorbeeld, Grondwettelijk Hof, arrest nr. 29/2018 van 15 maart 2018, punt B.18, en Grondwettelijk Hof, arrest nr. 44/2015 van 23 april 2015, punten B.36.1 e.v.

³³ Advies nr. 63.202/2 van 26 april 2018 van de Raad van State over een voorontwerp van wet «*tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van Verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG*», Parl.St. Kamer, 54-3185/001, pp. 121-122.

Zie in dezelfde zin de volgende adviezen van de Raad van State:

- Advies nr. 26.198/2, van 2 februari 1998, over een voorontwerp dat geleid heeft tot de wet van 11 december 1998 «*tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens*», Parl.St. Kamer 1997-1998, nr. 49-1566/1, blz. 201.
- Advies nr. 33.487/1 van 18 en 20 juni 2002 over een voorontwerp dat geleid heeft tot de wet van 22 augustus 2002 «*houdende maatregelen inzake gezondheidszorg*», Parl.St. Kamer 2002-2003, nr. 2125/2, blz. 539.
- Advies nr. 37.765/1/2/3/4, van 4 november 2004 over een voorontwerp dat geleid heeft tot de programmawet van 27 december 2004, Parl.St. Kamer 2004-2005, nr. 1437/2.

³⁴ Zie eveneens Grondwettelijk Hof, arrest nr. 29/2010 van 18 maart 2010, punt B.16.1 ; arrest nr. 39/2013 van 14 maart 2013, punt B.8.1 ; arrest 44/2015 van 23 april 2015, punt B.36.2 ; arrest nr. 107/2015 van 16 juli 2015, punt B.7 ; arrest nr. 108/2017 van 5 oktober 2017, punt B.6.4 ; arrest nr. 29/2018 van 15 maart 2018, punt B.13.1, arrest nr. 86/2018 van 5 juli 2018, punt B.7.2.: advies van de Raad van State nr. 63.202/2 van 26 april, punt 2.2.

doeleinden van de verwerking van persoonsgegevens) en de categorieën van persoonsgegevens die onderling worden gekoppeld (art. 9, §1, tweede lid), andere taken (d.w.z. mogelijk andere verwerkingsdoeleinden) van de LTF (art. 33, §2, in fine) en de modaliteiten voor de uitoefening van rechten inzake rectificatie, uitwissing of (indirecte) toegang (art. 40).

21. Aangezien dit essentiële elementen van de verwerking zijn, is de Autoriteit van mening dat de bepalingen van het ontwerpbesluit (en de overeenkomstige elementen van het Verslag aan de Koning) moeten worden opgenomen in het wetsontwerp (en in het commentaar bij de desbetreffende artikelen) en dat bijgevolg de delegaties in de artikelen 6, 9, 33 en 40 van het wetsontwerp uitdrukkelijk moeten worden beperkt tot de uitvoeringsmodaliteiten van de essentiële elementen, die bij wet moeten worden vastgesteld.

Speciale opmerking over logbestanden

22. Artikel 8 van het wetsontwerp heeft betrekking op de logbestanden van de verwerkingen van gegevens in de GGB. In het commentaar bij dit artikel staat dat deze bepaling een gewijzigde versie is van art. 44/4, §2, lid 2 WPA, in die zin dat de lijst van verwerkingen die het voorwerp moeten zijn van een logging exhaustief is. De Autoriteit is voorstander van een dergelijke uitputtende lijst, maar merkt op dat artikel 8, § 1, van het wetsontwerp de Koning machtigt om "*andere types*" verwerking te bepalen waarvoor logbestanden worden aangelegd. In dit verband is de Autoriteit, gezien de door de aanvrager geuite wens van exhaustiviteit, van mening dat deze machtiging moet worden weggelaten en dat *« elke verwerking van de gegevens in de gemeenschappelijke gegevensbank, met inbegrip van de registratie ervan, wordt onderworpen aan logging »*.
23. De Autoriteit merkt op dat de lijst in artikel 8, §1 geen melding maakt van het "extraheren" van lijsten (waarnaar wordt verwezen in artikel 26, §1) door diensten met een leesrecht, voor "interne verwerking". Deze bepaling stelt ook dat deze extractie - die de Autoriteit opvat als de mogelijkheid om gegevens van deze lijst te kopiëren - moet worden uitgevoerd door een personeelslid met een veiligheidsmachtiging van het niveau "geheim". De Autoriteit wijst erop dat het toezicht op de naleving van deze voorwaarde betekent dat de mogelijkheid van extractie door deze diensten wordt gekoppeld aan het bestaan van een wettelijke verplichting om deze extractie in een logbestand op te nemen (afdwingbaar tegen deze diensten³⁵).
24. In het commentaar bij artikel 8 wordt ook gespecificeerd dat "*de verzameling*" is vervangen door "*de opname van gegevens*" om de "*IT-reëliteit*" weer te geven. De Autoriteit begrijpt dat dit argument eigenlijk betekent dat de GGB niet verzamelt (en niet dat het een computersysteem en de werking

³⁵ Zie over deze kwestie *infra*.

ervan is dat bepaalt hoe een wettekst moet worden geformuleerd³⁶). In die zin, met de belangrijke kanttekening dat het vanuit het oogpunt van de verwerkingsverantwoordelijke is en niet vanuit het oogpunt van de gegevensbank³⁷, is de Autoriteit van mening dat dit argument toelaatbaar is. De effectiviteit van het principe van nauwkeurigheid van gegevens hangt echter in grote mate af van de mogelijkheid om de naleving van de regels voor gegevensbescherming te controleren zodra de gegevens worden verzameld (en op de plaats waar ze worden verzameld). De Autoriteit is daarom van mening dat moet worden bepaald dat het verzamelen van gegevens die waarschijnlijk in de GGB zullen worden geregistreerd, in een logbestand zijn opgenomen. De organieke normen van de diensten met schrijfrechten zullen daarom dienovereenkomstig moeten worden aangepast.

25. De Autoriteit is ook van mening dat dezelfde zorg voor doeltreffendheid betekent dat het ontwerp en de organieke normen van de partnerdiensten voor de "*lokale*" verwerking, de procedures (inclusief de frequentie) voor het controleren van de logbestanden moeten omvatten (hoewel de uitvoerende macht bevoegd kan zijn om dit te doen).
26. **Met het oog op de wijziging van de regels voor de partnerdiensten**, die nader zal worden toegelicht bij de analyse van de bepalingen betreffende de verwerkingsverantwoordelijken, moet worden opgemerkt dat de naleving van het legaliteitsbeginsel ook vereist dat aandacht wordt besteed aan de gepastheid van de doeleinden van de geplande verwerkingen in verhouding tot de **bevoegdheid van de wetgever**³⁸. De Autoriteit vestigt de aandacht van de aanvrager op het feit dat in het geval van een nieuwe staatshervorming de rechtmatigheid van de verwerking van in de GGB opgeslagen gegevens (en/of de verstrekking ervan) waarschijnlijk in het gedrang komt totdat een samenwerkingsakkoord is goedgekeurd.

II.2. Doeleinden.

27. Volgens artikel 5.1.b) van de AVG is een verwerking van persoonsgegevens enkel toegestaan voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Ook moet, overeenkomstig artikel 6.3 van de AVG, gelezen in het licht van overweging 41 van de AVG en artikel 22 van de Grondwet, het doel op voldoende uitdrukkelijke en nauwkeurige wijze worden geformuleerd, zodat voor de betrokkenen duidelijk is wat de precieze redenen zijn die tot de verwerking van hun persoonsgegevens hebben geleid. Uit de lezing van het doeleinde moet de burger kunnen opmaken welke gegevensverwerkingen nodig zijn om het doeleinde te realiseren.

³⁶ Wat natuurlijk niet toelaatbaar zou zijn.

³⁷ Zie over deze kwestie *infra*.

³⁸ Met betrekking tot de vraag naar (het ontbreken van) de bevoegdheid van de federale overheid om verplichtingen op te leggen aan alle overheden die toegang hebben tot gemeenschappelijke gegevensbanken, met inbegrip van die van de gefedereerde entiteiten, zie het advies van de afdeling Wetgeving van de Raad van State nr. 59.515/2 van 6 juli 2016 over een ontwerp van koninklijk besluit een ontwerp van koninklijk besluit betreffende de gemeenschappelijke gegevensbank foreign terrorist fighters en tot uitvoering van sommige bepalingen van de afdeling 1bis "het informatiebeheer" van hoofdstuk IV van de wet op het politieambt", punten 2.2. à 2.3.3. (<http://www.raadvst-consetat.be/dbx/avis/59515.pdf>)

28. Artikel 3 van het wetsontwerp omschrijft het algemene doel van de gegevensverwerking waarin het wetsontwerp voorziet, namelijk «*het bestrijden, voorkomen en opvolgen van terrorisme en extremisme wanneer dit tot terrorisme kan leiden*». Deze bepaling specificeert ook dat deze doelstelling wordt nagestreefd door de basisdiensten EN de partnerdiensten «*elk in het kader van zijn wettelijke bevoegdheden*».
29. In artikel 5 van het wetsontwerp worden de **4 specifieke doeleinden** «*van de GGB*» uiteengezet. Het gaat om (1) het gecoördineerde overleg tussen de basisdiensten en de partnerdiensten; (2) de strategische, tactische of operationele noodzaak om gezamenlijk persoonsgegevens en informatie te verwerken voor het uitoefenen van de respectievelijke opdrachten van de basisdiensten en de partnerdiensten; (3) de hulp bij het nemen van beslissingen door de bestuurlijke overheden of bij het nemen van beslissingen van bestuurlijke of gerechtelijke politie; (4) de analyse, de evaluatie en de opvolging, daaronder begrepen het nemen van maatregelen, van de in de gemeenschappelijke gegevensbank T.E.R. geregistreerde entiteiten en de analyse, de evaluatie en de opvolging van het fenomeen van terrorisme en extremisme wanneer het kan leiden tot terrorisme, op grond van een dreigingsevaluatie.
30. Ten eerste herhaalt de Autoriteit het verzoek dat de CBPL al in 2015 deed, namelijk dat strategische, tactische en operationele vereisten van elkaar worden onderscheiden en nauwkeurig worden beschreven in de wet of een uitvoeringsbesluit³⁹.
31. Daarnaast herhaalt de Autoriteit dat zij voorstander is van het vaststellen van de doeleinden van een gegevensbank (of register), maar dat het een feit blijft dat naleving van artikel 5.1.b) van de AVG (evenals artikel 28, 2° en artikel 75 van de WVG) vereist dat **de doeleinden van de verwerking** van persoonsgegevens worden vastgesteld (waarvan registratie in een specifieke gegevensbank slechts één voorbeeld is). Bijgevolg moet een onderscheid worden gemaakt tussen de doeleinden die verband houden met de oprichting van een gegevensbank en de doeleinden van de verschillende verwerkingshandelingen die door elk van de diensten met betrekking tot deze gegevens worden uitgevoerd (verzameling, raadpleging in LTF, registratie in GGB, mededeling aan andere diensten, internationale overdrachten, enz.).
32. Wat de verzameling betreft, wordt (in de toelichting) gewoon verwezen naar de organieke wetgeving van de basisdiensten en partnerdiensten. Anderzijds zal voor elke dienst met een schrijfrecht moeten worden aangetoond (in het commentaar bij artikel 6) hoe het doel van elke verdere verwerking van deze gegevens verenigbaar is met het doel waarvoor ze zijn verzameld.

³⁹ Advies 57/2007, *op. cit.*, punt 54.

33. Wat de verdere verwerking door de partnerdiensten betreft, staat artikel 6, §2, 2° van het wetsontwerp de verwerking toe van de operationele politiegegevens van de GGB «*die toereikend, ter zake dienend en niet overmatig zijn in het licht van de opdrachten [van het voorkomen en opvolgen van terrorisme en extremisme, wanneer dit kan leiden tot terrorisme (...)] van deze diensten, elk in het kader van zijn wettelijke bevoegdheden*» en de doeleinden [van de GGB]», door de basisdiensten en partnerdiensten met schrijfrecht⁴⁰.
34. De Autoriteit wijst erop dat het bepalen welke categorieën persoonsgegevens over entiteiten in de GGB rechtmatig toegankelijk zijn, d.w.z. aan partnerdiensten mogen worden meegedeeld (of zelfs eenvoudig in de GGB mogen worden opgevraagd), afhangt van zowel het bestaan van een rechtsgrondslag voor de verstrekking EN de specifieke doeleinden van deze partnerdiensten. Met andere woorden, ongeacht de technische beperkingen van de gegevensdrager⁴¹, **kan registratie in de GGB er niet toe leiden dat een dienst persoonsgegevens verwerkt (al is het maar door raadpleging) die hij op grond van zijn eigen doeleinden niet mag verwerken.**
35. Bijgevolg moeten zij ofwel (1) op grond van de verwerkingsdoeleinden waaraan zij krachtens hun organieke wetgeving onderworpen zijn, reeds toegang hebben tot deze gegevens (in dat geval moet worden verwezen naar de toepasselijke regels en moet in het commentaar bij artikel 6 worden gespecificeerd dat de ontwerpbepaling beperkt is tot het verschaffen van een technisch communicatiemiddel), ofwel (2) beoogt het ontwerp te voorzien in een nieuw toegangsdoel voor deze diensten (in dat geval moet uitdrukkelijk worden voorzien in een dergelijk toegangsdoel, dat gerechtvaardigd, noodzakelijk en evenredig moet zijn en de relevante organieke wetten moeten dienovereenkomstig worden gewijzigd), of ten slotte (3) is de aanvrager van mening dat de huidige mededeling, bijvoorbeeld in de vorm van een eenvoudig bericht (gunstig of negatief), een politierapport of een verzoek om maatregelen te nemen, te beperkt is en is hij van plan deze uit te breiden (en in dit geval moeten niet alleen de respectieve organieke wetten worden aangepast, maar moet ook het noodzakelijke en evenredige karakter van de toename van de hoeveelheid meegedeelde gegevens naar behoren worden aangetoond).
36. In voorkomend geval, en op voorwaarde dat het noodzakelijke en evenredige karakter van deze mededeling en/of toegang wordt aangetoond, moet het ontwerp voorzien in de aanpassing (geldig voor de toekomst) van de organieke normen van diensten waarvan het doel momenteel niet is aangegeven op een manier die een verenigbare verdere verwerking mogelijk maakt.

⁴⁰ Er dient opgemerkt te worden dat volgens het ontwerp van Koninklijk Besluit enkel de DG Veiligheid en Preventie, de DG Consulaire Zaken en de Dienst Erediensten en Vrijzinnigheid een bevraging (in de vorm van een hit - no hit) van de GGB kunnen doen, terwijl alle anderen leesrecht hebben.

⁴¹ Zie het voorbeeld hierboven over de Dienst Erediensten.

37. De Autoriteit specificeert dat de doeleinden van dergelijke toegang door partnerdiensten **voor elke gegevenscategorie** moeten worden vastgesteld. Er kan geen sprake van zijn, zoals de huidige formulering van art. 6, §2, 2° van het wetsontwerp doet vrezen, dat alles wordt meegedeeld⁴² en dat het aan de ontvangende overheden wordt overgelaten om te selecteren wat zij mogen raadplegen. De formulering van het ontwerp moet bijvoorbeeld duidelijk maken dat bepaalde categorieën van gegevens onder geen enkele omstandigheid kunnen worden meegedeeld (of toegankelijk gemaakt) aan de Algemene Administratie van de Thesaurie, of enkel de aanwezigheid van een entiteit.
38. Voor alle duidelijkheid wijst de Autoriteit erop dat doeleinden die gericht zijn op het gemakkelijker maken voor de basisdiensten of **doeleinden met budgettaire impact**, (bijvoorbeeld, in ruil voor het uitwisselen van gegevens die veel verder gaan dan wat de partnerdiensten voor hun taken mogen verwerken, zouden zij geen lijsten⁴³ meer hoeven door te geven of automatisch gegevens over entiteiten ontvangen, zonder deze bij de partnerdiensten⁴⁴ te hoeven verzamelen) **niet als legitiem kunnen worden beschouwd**⁴⁵.
39. De Autoriteit vermeldt terloops dat het stellen van grenzen of het vermelden in de toelichting van de omstandigheden waarin een verwerking onrechtmatig van het doeleinde zou afwijken, wel degelijk een goede praktijk is, met name wanneer - zoals hier het geval is - de inmenging bijzonder groot is of de risico's van misbruik groot zijn.
40. Wat de in artikel 9 van het wetsontwerp bedoelde **onderlinge koppeling** betreft, is de Autoriteit van oordeel dat moet worden bepaald dat de onderlinge koppeling van de GGB met authentieke bronnen er in geen geval toe mag leiden dat autoriteiten die geen legale toegang tot deze bronnen hebben, toegang krijgen tot de gegevens in deze authentieke bronnen. Deze voorzorgsmaatregel, die vereist

⁴² Het verslag van het Comité I bevestigt deze indruk door het volgende te stellen «*voor de inlichtingendiensten ligt het belang van de GGB in het feit dat ze op een enkele plaats alle informatie vinden waarover hun partners beschikken en via een enkel kanaal de niet-geclassificeerde informatie waarover ze beschikken, kunnen delen*» (Comité I, Toezichtonderzoek naar de opvolging door de Belgische inlichtingen- en veiligheidsdiensten van wegens terrorisme veroordeelde en/of geradicaliseerde gedetineerden, tijdens en na hun opsluiting, 31 mei 2022, blz. 19 (https://www.comiteri.be/images/pdf/enquetes/TERROR_PRISON_UNCLASS_NL.pdf)); Over de opportuniteit om beroep te doen op private set intersection, zie voetnoot 13 (*supra*).

⁴³ Zie het verslag van de Comités I en P over het Toezichtsonderzoek naar de ondersteunende diensten van het OCAD *dat stelde dat «vroeger, het OCAD elke maand aan de Dienst Erediensten en Vrijzinnigheid (DG WL) een lijst stuurde van personen van wie het vaststaat dat ze haatpropagandisten zijn. De Dienst vergeleek deze lijst met de weddestaten van de bedienaars van de erediensten en van de afgevaardigden van de Centrale Vrijzinnige Raad. Tegenwoordig heeft de Dienst toegang tot de Gemeenschappelijke gegevensbank.* (op.cit., blz 24).

⁴⁴ Zie het verslag van het Comité I dat het volgende stelt «*oor de inlichtingendiensten ligt het belang van de GGB in het feit dat ze op een enkele plaats alle informatie vinden waarover hun partners beschikken (...)*», Comité I, Toezichtonderzoek naar de opvolging door de Belgische inlichtingen- en veiligheidsdiensten van wegens terrorisme veroordeelde en/of geradicaliseerde gedetineerden, tijdens en na hun opsluiting, op.cit. blz 18).

⁴⁵ Het Hof van Justitie oordeelt inderdaad dat «*de omstandigheid dat aan overheidsinstanties te weinig middelen worden toegekend, in geen geval een legitieme reden kan vormen die vermag te rechtvaardigen dat inbreuk wordt gemaakt op de door het Handvest gewaarborgde grondrechten*» (HvJEU, 1 augustus 2022, C 184/20, OT vs. Vyriausioji tarnybinės etikos komisija, § 89).

is omdat werd gekozen voor centralisering in plaats van de invoering van een kruispuntbanksysteem⁴⁶, is ook in overeenstemming met het standpunt dat het een goede praktijk is om grenzen te stellen of in de memorie van toelichting de omstandigheden te vermelden waarin een verwerking misbruik van het doel zou vormen.

Opmerkingen in verband met de LTF

41. Art. 31 e.v. van het wetsontwerp voorzien in (of wijzigen) de gegevensverwerking tijdens het LTF-overleg. Hoewel deze bepalingen bepaalde opmerkingen oproepen, wil de Autoriteit duidelijk maken dat **zij zeer positief staan tegenover het wetgevingskader voor gegevensverwerking tijdens het LTF-overleg.**
42. Wat de doeleinden van de verwerkingen betreft, bepaalt art. 31 van het wetsontwerp dat de relevante persoonsgegevens worden uitgewisseld binnen één of meer overlegplatforms die binnen elk gerechtelijk arrondissement worden opgericht, de zogenaamde LTF «met het oog op de verrijking van persoonsgegevens en informatie met betrekking tot entiteiten, alsmede het monitoren van en het ondernemen van actie met betrekking tot entiteiten die in de [GGB] zijn gevalideerd».
43. Terwijl artikel 31 van het wetsontwerp het doel van het verrijken van de GGB⁴⁷ lijkt te benadrukken, begrijpt de Autoriteit bij het lezen van de toelichting dat deze bepaling meer bedoeld is, in een *post-Conings* context⁴⁸, om te voorzien in een verplichting van "loyale" uitwisseling van gegevens ("geclassificeerd" of niet), betreffende "dit bijzonder ernstig fenomeen", van diensten die nodig zijn om de GGB te voeden of niet. Het bijkomstige karakter van de verrijking van de GGB lijkt te worden bevestigd door de passage in het commentaar die stelt dat «*zolang deze informatie echter geclassificeerd of vertrouwelijk is, zal ze niet in de verslaggeving van de lokale task forces kunnen vermeld worden*»⁴⁹.
44. De huidige formulering van artikel 31 komt erop neer dat een gegevensverwerking (uitwisseling) wordt gerechtvaardigd door een andere gegevensverwerking (registratie). Deze bepaling moet daarom worden geherformuleerd om ze in overeenstemming te brengen met het commentaar (bv. door de "gegevensbank"-benadering te verlaten, d.w.z. door registratie in de GGB te beschouwen als een van

⁴⁶ De Autoriteit beweert niet dat dit niet te bekritisieren valt

⁴⁷ Ongetwijfeld omdat het hoofdstuk 3 opent met de titel «Verrijking van gegevens over entiteiten en opvolging van een in de gemeenschappelijke gegevensbank T.E.R. gevalideerde entiteit».

⁴⁸ Zie voor deze kwestie hierna het onderzoek van de proportionaliteit.

⁴⁹ Met andere woorden, ze kunnen niet worden opgenomen in de GGB voordat ze gedeclineerd zijn.

de verwerkingshandelingen die waarschijnlijk zullen worden uitgevoerd met het oog op raadpleging in LTF).

45. In het inleidende commentaar bij hoofdstuk 3 wordt gespecificeerd dat «*het resultaat van dit overleg wordt overgezonden aan de bevoegde overheid om te beslissen over de betrokken maatregel*» en in het commentaar bij artikel 31 wordt hieraan toegevoegd «*de diensten zijn ertoe gehouden enkel de persoonsgegevens en de informatie uit te wisselen waarvoor zij het recht hebben ze te verwerken in het kader van hun opdrachten*»⁵⁰.
46. De doeleinden van de gegevensmededeling aan de diensten die worden uitgenodigd om deel te nemen aan de LTF, overeenkomstig artikel 32 van het wetsontwerp, moeten zodanig worden geformuleerd dat de betrokken personen, maar ook de deelnemers, bij lezing ervan kunnen weten of de uitnodiging van de "*uitgenodigde diensten*" beperkt is tot het verzoek de gegevens waarover zij beschikken mee te delen en/of bepaalde maatregelen te nemen, dan wel of (en zo ja, in welke omstandigheden) de doeleinden van de gegevensverwerking in het kader van de LTF's, in combinatie met de taken en de "*need to know*" van de uitgenodigde diensten, rechtvaardigen dat bepaalde categorieën gegevens (die ten minste bepaalbaar moeten zijn) aan de uitgenodigde diensten worden meegedeeld.
47. Het zal ook nodig zijn om duidelijk te bepalen of de LTF's **georganiseerde overlegplatforms zijn in de zin van artikel 458ter van het Strafwetboek**. Indien dit het geval is, zal hoofdstuk 3 in zijn geheel moeten worden herzien om het doel nauwkeurig te bepalen (en *in concreto* de noodzakelijkheid en evenredigheid van de beoogde verwerking aan te tonen)⁵¹. **Indien nodig zou de Autoriteit, gezien het belang van de vereiste wijzigingen, graag zien dat het gewijzigde ontwerp opnieuw voor advies aan haar wordt voorgelegd voordat het wordt goedgekeurd.**

Doeleinde van het recht op mededeling van bepaalde categorieën persoonsgegevens die onder het beroepsgeheim vallen⁵²

48. Artikel 19, 3de lid van het ontwerp bepaalt «*Artikel 458 van het Strafwetboek kan niet ingeroepen worden wanneer een basisdienst of een partnerdienst in het kader van de bepalingen in deze afdeling haar schrijfrecht itoefent in de gemeenschappelijke gegevensbank T.E.R.*» Het commentaar bij dit artikel preciseert «*Het artikel bepaalt ook dat artikel 458 van het Strafwetboek betreffende de schending van het beroepsgeheim in deze context niet kan worden opgeworpen tegen de basisdiensten*

⁵⁰ De Franse versie bepaalt "*les services sont tenus de n'échanger que les données à caractère personnel et les informations qu'ils ont le droit de traiter dans le cadre de leurs missions*"

⁵¹ Zie hierover de opmerkingen van de Autoriteit in haar advies 254/2022 van 1 december 2022 (<https://www.autoriteprotectiondonnees.be/publications/avis-n-254-2022.pdf>); Voor het onderzoek van de proportionaliteit, zie hierna.

⁵² De Autoriteit wijst erop dat, ongeacht het beroepsgeheim, de GGB moet worden gevoed op basis van een wettelijke verplichting die uitgaat van een **wetgever die bevoegd is** om een verplichting vast te stellen die aan de betrokken autoriteiten kan worden opgelegd.

of partnerdiensten die de gemeenschappelijke gegevensbank T.E.R. voeden via hun schrijfrecht». De Autoriteit leidt uit de toelichting af dat deze bepaling niet bedoeld is om te voorkomen dat diensten zich op het beroepsgeheim beroepen om zich tegen de voeding van de GGB te verzetten, maar om ervoor te zorgen dat de voeding nooit als een schending van het beroepsgeheim kan worden beschouwd.

49. Als deze interpretatie juist is, komt dit neer op het creëren van een nieuwe wettelijke uitzondering op het beroepsgeheim en zou het wenselijk zijn dat het ontwerp het Strafwetboek wijzigt om dit nieuwe type uitzondering in te voeren. Als dit het geval is, is het echter raadzaam om **de logica van gegevensbanken los te laten**. Door de uitzondering enkel te laten hangen van de "*uitoefening van het schrijfrecht*" door de basis- of partnerdiensten⁵³ en door geen precieze voorwaarden voor de toepassing van deze uitzondering vast te leggen, dreigt het ontwerp er immers toe te leiden dat zelfs informatie waarvan de mededeling totaal nutteloos zou zijn voor de in art. 3 van het wetsontwerp vermelde doeleinden, niet meer zal worden meegedeeld aan de deelnemers die onderworpen zijn aan het beroepsgeheim uit vrees voor de openbaarmaking ervan. Bovendien is een duidelijke definitie van het doeleinde van het recht om bepaalde categorieën persoonsgegevens mee te delen die onder het beroepsgeheim vallen, een maatregel die zowel de betrokkene als de deelnemende beroepsbeoefenaar beschermt⁵⁴. Bij het herformuleren van het commentaar bij artikel 19 moet er daarom op worden gelet dat de bepaling niet zodanig wordt geïnterpreteerd dat dit negatieve gevolgen kan hebben voor het functioneren van een instelling die geheimhouding beoogt te beschermen.
50. Als de uitzondering op het beroepsgeheim bedoeld is om een antwoord te bieden op het probleem dat is ontstaan door de dood van politieagent Thomas Monjoie⁵⁵, moet vooral worden bepaald wat de ontvanger van informatie die onder het beroepsgeheim valt, kan en/of moet doen met de verstrekte gegevens. Als de persoon door de politie als gevaarlijk wordt beschouwd, kan deze informatie alleen worden gebruikt om aan het medisch personeel te rechtvaardigen dat de politie ter plaatse blijft om de bescherming van het medisch personeel te garanderen. Indien de medische staf, ongeacht de gevaarlijkheid, in kennis moet worden gesteld van factoren op grond waarvan psychische stoornissen kunnen zijn vermoed (zoals verklaringen dat de betrokkene van plan was politieagenten aan te vallen),

⁵³ Naar analogie betekent dit dat een reddingsvoertuig nooit geacht kan worden een overtreding van de verkeersregels te begaan.

⁵⁴ Na het lezen van dit doel zou de beoefenaar in staat moeten zijn om vragen te beantwoorden van het type die door prof. Jacques Fierens zijn gesteld en die voorkomen in de notulen van "la journée de réflexion" van 30 januari 2018 met als titel "*Le secret professionnel en danger - la concertation de cas en question*", blz. 21 en 22 (https://www.liquedh.be/wp-content/uploads/2018/11/Etude_LDH_DOSSIER_458TER_avril_2018.pdf); Zie hierover eveneens de opmerkingen van de Autoriteit in haar advies 254/2022 van 1 december 2022 (<https://www.autoriteprotectiondonnees.be/publications/avis-n-254-2022.pdf>).

⁵⁵ Waarvan sprake is in de memorie van toelichting (blz. 6); Over deze kwestie, zie Commissie Justitie en Binnelandse Zaken, 14 november 2022, Com 929, blz. 2 ev. (<https://www.lachambre.be/doc/ccra/pdf/55/ac929.pdf>)

moet worden bepaald aan welke verplichting de medische staf op grond van deze informatie zou zijn onderworpen. Enerzijds kan de persoon die de vertrouwelijkheid heeft meegedeeld de noodzakelijke geheimhouder van zijn verplichting ontslaan en anderzijds heeft in deze zaak de medische staf geen bezwaar gemaakt tegen de vrijwillige internering. Hij had gewoonweg geen tijd om zich over de betrokken persoon te ontfemen, die zonder toezicht werd achtergelaten, voordat hij uit de wachtkamer verdween⁵⁶. Bijgevolg moet het doel van de door de aanvrager beoogde gegevensverwerking in een geval als dit zodanig worden gespecificeerd dat kan worden aangetoond dat het noodzakelijk en evenredig is.

51. Bovendien merkt de Autoriteit op dat deze bepaling, zoals zij momenteel is geformuleerd, alleen van toepassing is op noodzakelijke geheimhouders van informatie die onder een geheim valt waarop 458 van toepassing is (in tegenstelling tot het onderzoeksgeheim⁵⁷, de geheimhoudingsplicht of de geheimhoudingsplicht die voortvloeit uit de statuten of zelfs uit een contract⁵⁸ waarvan het sluiten een voorwaarde zou zijn die is vastgesteld door de wet⁵⁹ om bepaalde taken te kunnen uitvoeren of toegang te kunnen krijgen tot bepaalde gegevens).
52. Bovendien vallen binnen de lijst van partnerdiensten waarschijnlijk alleen bepaalde werknemers binnen de jeugdzorg, de justitiehuisen en de gezondheidswerkers en maatschappelijk werkers in dienst van VZ onder de geheimhoudingsplicht waarnaar wordt verwezen in artikel 458 van het Strafwetboek. Wat hen betreft, verzet artikel 458 van het strafwetboek zich er echter tegen dat informatie die onder de geheimhoudingsplicht valt, wordt meegedeeld aan hun directie, die niet onder het beroepsgeheim valt (en dus geen geheimhoudingsplicht zou schenden door aan de GGB te leveren). Indien de aanvrager voornemens is deze bepaling op andere partijen en/of autoriteiten toe te passen, moet in de toelichting bij artikel 19 bijgevolg worden gespecificeerd welke partijen en op welke wijze.
53. Wat het beroepsgeheim van de deelnemers aan een **LTF-raadpleging** betreft, verbaast het de Autoriteit dat, hoewel het voorlaatste lid van artikel 32, §1, van het wetsontwerp uitdrukkelijk voorziet in de mogelijkheid dat andere departementen, organen of instanties worden uitgenodigd om deel te nemen aan een LTF, niet is voorzien in een afwijking van artikel 458 van het Strafwetboek. In voorkomend geval wordt **het doel van het recht om bepaalde categorieën persoonsgegevens mee te delen** die onder het beroepsgeheim vallen, duidelijk omschreven. Immers, zoals het College

⁵⁶ *Ibidem*, blz. 7 ev.

⁵⁷ Waarvan overigens specifiek sprake is in het volgende lid.

⁵⁸ Of het nu een arbeidsovereenkomst of een NDA betreft.

⁵⁹ Als gevolg hiervan zou een eenvoudige redenering in termen van de hiërarchie van normen de wettelijke verplichting zinloos maken.

van procureurs-generaal aangeeft (met betrekking tot LVIC)⁶⁰, « *Degene die zijn beroepsgeheim schendt omdat hij bij gelegenheid van het overleg geheimen toevertrouwt die geen betrekking hebben op de misdrijven waarvoor het overleg werd georganiseerd (...) zou in beginsel strafrechtelijk vervolgd kunnen worden. (...) . Er moet bijgevolg over gewaakt worden dat een eventuele mededeling van geheimen steeds plaats vindt binnen het vooropgestelde doel en overeenkomstig de vastgelegde modaliteiten van het overleg* »⁶¹. Als gevolg hiervan kunnen **de gegevens van deelnemers worden verwerkt voor handavingsdoeleinden**. Uiteraard worden de wezenlijke elementen van een dergelijke verwerking beschreven in het Wetboek van Strafvordering. Niettemin is de Autoriteit van mening dat het ontwerp de aandacht van de deelnemende beroepsbeoefenaren moet vestigen op de mogelijkheid dat hun gegevens voor een dergelijk doel worden verwerkt.

Doeleinde van gearcheiverde gegevens

54. Het commentaar bij artikel 4 preciseert « *in tegenstelling tot wat nu in de wet op het politieambt is bepaald, is de zin 'zonder afbreuk te doen aan de wet van 24 juni 1955 betreffende de archieven' geschrapt omdat die verwijzing al in artikel 7 staat, waar ze relevanter is. De archiefwet heeft immers betrekking op de archivering en de uitwissing van persoonsgegevens en vormt zelfs een uitzondering op het beginsel van de verwijdering* ». Artikel 7, §2, eerste lid van het wetsontwerp voorziet echter niet in archivering overeenkomstig de archiefwet van 24 juni 1955. Deze wet wordt alleen genoemd in lid 2, waarin staat dat « *na afloop van deze termijn, worden deze gegevens en informatie gewist onverminderd de archiefwet van 24 juni 1955* ».
55. Bijgevolg blijven deze gegevens, die moeten worden gearcheiverd « *ten laatste 30 jaar na de laatste verwerking* » (art. 7, §1) en waarvan de verwerkingsdoeleinden « *de verwerking van de antecedenten in het kader van een gerechtelijk onderzoek of inlichtingenonderzoek met betrekking tot een terrorisme en extremisme dat tot terrorisme kan leiden* » (art. 7, §2, 2°) in handen van de verwerkingsverantwoordelijke in een vorm die identificatie mogelijk maakt⁶².

⁶⁰ Zie *infra*.

⁶¹ COL 04/2018 van 15 maart 2018, bl. 14 (https://www.om-mp.be/sites/default/files/u1/col04_2018_casusoverleg_nl.pdf), de omzendbrief beveelt overigens aan om erover te waken dat « *alle deelnemers aan het overleg hierop gewezen worden vooraleer het overleg aan te vatten* » ; Zie in dit verband ook de verduidelijkende nota van OCAD over LVC-R, blz. 6 (https://ocad.belgium.be/wp-content/uploads/2020/09/verduidelijkende_nota_LVC-R-web.pdf) alsook advies 163 van 1 oktober 2018 van de "Conseil communautaire de l'aide à la jeunesse" (https://www.aidealajeunesse.cfwb.be/index.php?eID=tx_nawsecuredl&u=0&g=0&hash=b76aa4435faee9de86302b2c3552dd127cbb0a21&file=fileadmin/sites/ajss/upload/ajss_super_editor/DGAJ/Documents/CCAJ/Avis_163-CCAJ-Avant-projet_de_decret_concertation_de_cas-041018.pdf).

⁶² Enkel het resultaat van de exploitatie van archieven ter ondersteuning van de bepaling en uitvoering van het veiligheidsbeleid inzake terrorisme en extremisme dat zou kunnen leiden tot terrorisme wordt geanonimiseerd (art. 7, §2, derde lid, 5°), zonder dat de anonimiseringsstrategie wordt gespecificeerd in het commentaar

56. Hoewel het mechanisme van deze archivering sui generis (ook aanbevolen door de CBPL⁶³) begrijpelijk werd gemaakt door de toelichting die hierover werd gegeven in de parlementaire werkzaamheden met betrekking tot de wet van 18 maart 2014 betreffende het beheer van de politiegegevens⁶⁴, bemoeilijkt de omzetting van deze bepalingen in dit nieuwe wetsontwerp de beoordeling van de rechtmatigheid van de verwerking van de gearchiveerde gegevens.
57. Aangezien de verwijdering van gegevens wordt voorafgegaan door een lange archiveringsperiode (die zelf volgt op een lange bewaarperiode⁶⁵), kunnen bepaalde gearchiveerde persoonsgegevens worden bewaard in een vorm die het mogelijk maakt om ze te identificeren in de archieven van de GGB nadat ze zijn verwijderd door de verwerkingsverantwoordelijke die ze heeft verzameld. Hieruit volgt de noodzaak om, met betrekking tot het archiveringsdoeleinde (op zijn minst) een verwijzing op te nemen naar de voorbereidende werkzaamheden van de wet van 2014, in het commentaar bij artikel 7 en, met betrekking tot het doeleinde van de verwerking van gearchiveerde gegevens, het rechtmatige karakter ervan aan te tonen in het licht van de "alarmerende" bevinding van het COC⁶⁶ over de kwaliteit van een andere gegevensbank beheerd door de GGB-beheerder en de relevante jurisprudentie⁶⁷.
58. De Autoriteit merkt op dat de artikelen 4, 24, 46 en vooral artikel 28⁶⁸ van het wetsvoorstel verwijzen naar mogelijke verdere verwerking. De Autoriteit wijst er alleen op dat persoonsgegevens niet verder mogen worden verwerkt op een manier die onverenigbaar is met de doeleinden waarvoor ze zijn verzameld. De Autoriteit herinnert aan het arrest 29/2018 waarin het Grondwettelijk Hof stelde dat de vereiste van een precieze, voorzienbare wettelijke grondslag (en dus een helder doeleinde) *"des te meer [geldt] wanneer persoonsgegevens door overheidsdiensten verder worden verwerkt voor andere*

⁶³ Advies 57/2015, op.cit., punt 63

⁶⁴ Wet van 5 maart 1992 betreffende het politieke informatiebeheer en tot wijziging van de wet van 5 augustus 1992 op het politieambt, de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en het Wetboek van strafvordering (BS 28.03.2014), zie Parl.St. 4 november 2013, 53-3105/001, blz. ev. <https://www.dekamer.be/FLWB/PDF/53/3105/53K3105001.pdf>.)

⁶⁵ Met uitzondering van de entiteiten in "vooronderzoek", gedefinieerd als entiteiten die op het moment van registratie in de GGB niet voldoen aan de criteria om als dergelijke entiteiten te worden beschouwd en die na 6 maanden worden gearchiveerd (en niet verwijderd).

⁶⁶ COC, *Jaarverslag 2020*, bl. 16 ev., beschikbaar op (https://www.controleorgaan.be/files/Activiteitenverslag_COC_2020_N.pdf): « (we) stellen (...) vast dat van de in 2020 behandelde ANG dossiers zo'n **75,69% (109 op 144 beslissingen)** aanleiding hebben gegeven tot een gehele of gedeeltelijke archivering/wissing van de politieke registraties in de ANG. In vergelijking met 2019 is dat percentage dus nog substantieel gestegen van 52% naar 75,69% (...)

Het is zonder meer een alarmerend cijfer dat bevestigt wat het Controleorgaan doorheen haar werking vaststelt. De kwaliteit (juistheid en nauwkeurigheid) van de politieke databanken laat nog (te) veel te wensen over. Dit is geen onschuldige vaststelling: burgers worden rechtstreeks of onrechtstreeks benadeeld door onjuiste, achterhaalde of anderszins niet correcte gegevensverwerkingen. Rechtstreeks omdat een politieke bejegening van de burger op grond van foute informatie (fouilleren, arrestatie, wijze van politieke benadering, koppeling met ANPR technische gegevensbanken, enz. ...) navenant is. Onrechtstreeks doordat de toegang tot bv. bepaalde beroepen ten onrechte wordt afgesloten of beëindigd: bewakingsagent, militair, private onderzoeker, werknemer in een kerncentrale, enz. ... worden allen beoordeeld op hun louter 'politieke verleden'.

⁶⁷ Grondwettelijk Hof, arrest 108/2016 van 14 juli 2016 (<https://www.const-court.be/public/n/2016/2016-108n.pdf> EHRvM, grote kamer, 4 december 2008, S. en Harper vs.. Verenigd Koninkrijk, § 103. 18 april 2013, M.K. vs Frankrijk, § 3; 17 december 2009, B.B. vs Frankrijk, § 61; 18 september 2014, Brunet vs. Frankrijk, §§ 35-40.

⁶⁸ Met betrekking tot de mededeling aan buitenlandse diensten en de daaropvolgende verwerking van deze gegevens door deze diensten.

*doeleinden dan die waarvoor ze oorspronkelijk werden verkregen*⁶⁹. Met andere woorden **moet de formulering van het doel van de verdere verwerking** (in dit geval het doel van de mededeling aan buitenlandse diensten) **het ook mogelijk maken de verenigbaarheid met het doel waarvoor de gegevens oorspronkelijk zijn verzameld, vast te stellen**.

59. Om redenen die *infra*⁷⁰ nader zullen worden toegelicht, is de Autoriteit van mening dat het passend is te vermelden (in artikel 4 van het ontwerp) **dat statistieken zullen worden opgesteld met het oog op de publicatie van een evaluatieverslag** (met in het ontwerp vast te stellen tussenpozen, maar ten minste om de drie jaar) over de doeltreffendheid van de toegepaste verwerkingsmethoden en de autoriteiten die bij het wetsontwerp en het uitvoeringsbesluit betrokken zijn in verband met de doeleinden waarvoor de gegevens in de GGB zijn opgeslagen.
60. De Autoriteit neemt deze gelegenheid te baat om erop te wijzen dat de productie van statistieken geen doel is in de zin van artikel 5.1.b) van de AVG (noch van de overeenkomstige bepalingen van de titels II en III van de WVG). In werkelijkheid betekent het produceren van statistieken het verwerken van gegevens voor een doel dat specifiek, expliciet en legitiem moet zijn (wat in dit geval de evaluatie van de wet is).

Opmerkingen over de LVIC-R

61. De Autoriteit merkt op dat, hoewel de toelichting (met name de artikelen 31 en 32) verwijzingen bevat naar de LVIC-R's, de ontwerpen zelf niet voorzien in gegevensverwerkingen verricht door de LVIC-R's⁷¹. Indien het wetsontwerp de gegevensverwerking door LVIC-R mogelijk wil maken (met inbegrip van het verzamelen van door LTF's doorgestuurde gegevens en het doorgeven van gegevens aan LTF's), moeten de essentiële elementen van deze verwerking in het wetsontwerp worden vastgesteld. Als dit niet de bedoeling is van de aanvrager, moet voor de duidelijkheid in het commentaar worden vermeld dat het ontwerp niet de rechtsgrondslag vormt voor de gegevensverwerking door de LVIC-R (en idealiter moet deze rechtsgrondslag worden geïdentificeerd⁷²).
62. Aan de andere kant, als het de bedoeling van de aanvrager is om de gegevensverwerking door de LVIC-R's te beperken tot doeleinden die verband houden met "sociale preventie" (zoals vermeld in het commentaar bij artikel 31), moet dit uitdrukkelijk in het wetsontwerp worden vermeld. In feite werken de LVIC-R's momenteel NIET ALLEEN op het niveau van sociale preventie (aangezien ze een

⁶⁹ Grondwettelijk Hof, arrest van 15 maart 2018, B.18.

⁷⁰ Zie het proportionaliteitsonderzoek.

⁷¹ Enkel het verslag aan de Koning betreffende artikel 3 van het ontwerp van KB vermeldt «*Die kinderen zouden dus eventueel aan bod kunnen komen in de LIVC-R en de sociopreventieve diensten zouden indien nodig een begeleiding kunnen opstarten.*»

⁷² De normen die de essentiële elementen van de verwerking bevatten, mogen niet worden verward met de norm die de LIVC-R opricht.

component bevatten voor de vroegtijdige detectie van personen in een proces van radicalisering (of dat er tekenen zijn die erop wijzen dat ze in een proces van radicalisering zitten))⁷³ en anderzijds maakt de notie van een "*veiligheidsperspectief*" van de LTF's het niet mogelijk om een grotendeels preventieve dimensie uit te sluiten (aangezien de verwerkte gegevens niet beperkt zijn tot gegevens met betrekking tot misdrijven)⁷⁴.

63. Voor alle duidelijkheid wijst de Autoriteit erop dat de preventieve functie van de LVIC-R's⁷⁵ momenteel wordt gespecificeerd in de voorbereidende werkzaamheden voor de wet van 30 juli 2018 **tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme**⁷⁶ (hierna "LVIC-wet") in deze termen : «*De LIVC's R zijn een instrument in de bestrijding van gewelddadige radicalisering doordat zij personen die zich in een radicaliseringsproces bevinden vroeg detecteren en geïndividualiseerde opvolgtrajecten kunnen uitwerken voor hen. (...) Daar waar een LTF focust op een reactieve en repressieve aanpak via een politionele en gerechtelijke opvolging (...), benadert een LIVC R de persoon vanuit het verhaal van de inclusieve samenleving. Dit weerspiegelt zich in de samenstelling van de overlegstructuren. (...) In een LIVC R daarentegen zetelen voornamelijk lokale maatschappelijke actoren. Met uitzondering van de lokale politie (Information Officer) die de link verzekert met de LTF, zetelt geen enkel lid van de LTF in de LIVC R* »⁷⁷. De Information Officer van de lokale politie is verantwoordelijk voor het delen van informatie tussen de LTF en de LVIC- R⁷⁸.

Doeleinden van de informatie van «*andere bestemmingen* »

64. Krachtens artikel 24 van het wetsontwerp kan een informatiekaart⁷⁹ worden meegedeeld «*aan een derde overheid of instelling die de behoefte om te kennen heeft (...)* ». Het commentaar bij deze bepaling geeft een voorbeeld van de gegevensmededeling «*aan een sociaal werker of aan een schooldirecteur met als doel het vertrek naar Syrië van een jongere die sociaal ontheemd is, te voorkomen*» of zelfs de burgemeester.

⁷³ Zie OCAD, Plan R, Verduidelikend nota over LIVC-R, december 2019, F. XAVIER, *L'accroissement du rôle du bourgmestre dans les matières liées à la sécurité, spécialement en ce qui concerne le radicalisme, l'extrémisme violent et le terrorisme*, Rev. dr. communal, 2021/2.

⁷⁴ «*Personen die geen strafbaar feit hebben gepleegd, kunnen worden opgenomen in deze gezamenlijke gegevensbank, die een preventieve functie heeft.*»

(<https://www.lachambre.be/doc/ccra/pdf/55/ac929.pdf>, blz. 23)

⁷⁵ Art. 2 van de LVIC-wet.

⁷⁶ BS 14.09.2018.

⁷⁷ Parl. St., Kamer, 2017-2018, 54-3209/001, blz. 4.

⁷⁸ Ibid, blz. 8, zie ook artikel 4 van de LVIC-wet.

⁷⁹ Het betreft «*fiche van een entiteit die een uittreksel van de inlichtingenfiche vormt, en die de persoonsgegevens en informatie bevat die strikt beperkt zijn tot de behoefte om te kennen van de bestemming, voor de opvolging van de entiteiten*»(art. 2, 10° van het wetsontwerp). Opgemerkt moet worden dat de toelichting op de informatiekaart abusievelijk onderscheid maakt tussen persoonsgegevens en dreigingsanalyse, de verbanden met andere entiteiten, aliases en toegepaste maatregelen, die ook persoonsgegevens zijn.

65. Ten eerste wijst de Autoriteit erop dat het beginsel van mededeling op een "behoefte om te kennen"-basis een beoordeling impliceert op basis van (categorieën van) gegevens en niet op basis van een drager als geheel (de informatiekaart). Opgemerkt dient te worden dat de Autoriteit vraagtekens plaatst bij de relevantie van⁸⁰ een evaluatie van de mededeling door beide basisdiensten EN door twee diensten die zelf als basisdiensten worden beschouwd.
66. Ten tweede vraagt de Autoriteit zich af of het voorbeeld van de sociale werker of schooldirecteur verenigbaar is met het begrip van een derde "*overheid*" of "*instelling*". De Autoriteit is echter van mening dat deze bestemmelingen indirect kunnen worden benaderd als de bestemming de verantwoordelijke voor de verwerking is voor een raadpleging in LIVC-R (wat volgens de Autoriteit de burgemeester zou moeten zijn). Art. 24 van het wetsontwerp en het bijbehorende commentaar moeten daarom worden geherformuleerd.
67. Wat de burgemeester betreft, merkt de Autoriteit op dat zijn informatie ook onder artikel 12 van het ontwerpbesluit valt. Het is echter niet duidelijk welke bepaling van de wet de Koning machtigt om de doeleinden van deze mededeling te specificeren. Om de rechtsgrondslag en de grenzen van deze machtiging duidelijk aan te geven, moeten deze bepalingen in het wetsontwerp worden vermeld.
68. Bovendien wordt in de toelichting bij art. 24 van het ontwerp een onderscheid gemaakt tussen een mededeling aan de burgemeester (1) via de korpschef, en « *is het de bedoeling om de burgemeester zo snel mogelijk te informeren, zelfs als de beschikbare informatie nog niet volledig is* » en deze (2) via « *de* »⁸¹ informatiekaart « *zodat hij de maatregelen kan nemen waarvoor hij bevoegd is* ». Artikel 12 van het wetsontwerp verduidelijkt dat de burgemeester de bestemming is van « *de* » informatiekaart betreffende de entiteiten « *die hun verblijfplaats of woonplaats in zijn gemeente hebben, zijn gemeente regelmatig bezoeken of er regelmatig activiteiten organiseren* » met uitzondering van de HP die worden beperkt tot diegenen « *van wie de effecten zichtbaar zijn in zijn gemeente of die hun verblijfplaats of woonplaats hebben in zijn gemeente, die zijn gemeente regelmatig bezoeken, of die er regelmatig een of meerdere activiteiten organiseren of plannen te organiseren* ». Artikel 12, § 2 verduidelijkt « *Zonder de operationele noodzaken in gevaar te brengen, en na contact met de korpschef van de politiezone die hem de informatiekaart toezond, gebruikt de burgemeester de persoonsgegevens en de informatie van de informatiekaart in het kader van zijn wettelijke bevoegdheden en onder zijn eigen verantwoordelijkheid* ». (...) Uit het Verslag aan de Koning blijkt dat met "gebruiken" moet worden begrepen « *informatiedeling* » « *met de verschillende lokale actoren die de behoefte hebben om te kennen* » en dat « *in het kader van zijn wettelijke bevoegdheden* » enerzijds doelt op zijn bevoegdheid

⁸⁰ Na evaluatie door de beheerder, de operationeel verantwoordelijke en de basisdiensten, kan een informatiekaart worden meegedeeld aan een derde overheid of instelling die de behoefte om te kennen heeft

⁸¹ Angezien deze kaart gemodificeerd moet kunnen worden, verdient het de voorkeur om "een" informatiekaart te vermelden.

«zoals wettelijk bepaald in de nieuwe gemeentewet (...) op het vlak van het voorkomen van terrorisme» en anderzijds zijn hoedanigheid van «overheid van bestuurlijke politie» krachtens dewelke «hij tevens op de hoogte (moet) gehouden worden van de concrete opvolging van sommige aan zijn gemeente verbonden entiteiten ».

69. De Autoriteit merkt op dat, hoewel artikel 12, § 2 van het ontwerpbesluit systematisch voorafgaand contact met de korpschef vereist, het verslag aan de Koning dit alleen vereist «*wanneer twijfel bestaat over het in gevaar brengen van een operationele opdracht*». Deze bepaling (of het verslag) zal dus moeten worden aangepast. Bij deze gelegenheid zal de mogelijkheid van mededeling "onder zijn verantwoordelijkheid" worden verduidelijkt, zodat deze bepaling niet kan worden geïnterpreteerd als een "clausule die de verantwoordelijkheid beperkt" van de verwerkingsverantwoordelijken van de GGB voor de mededeling van persoonsgegevens met het oog op verwerking voor doeleinden die niet gespecificeerd, uitdrukkelijk omschreven en gerechtvaardigd zijn. Opgemerkt moet worden dat een dergelijke clausule niet effectief zou zijn, omdat het in strijd zou zijn met hiërarchisch hogere normen.
70. Het is daarom essentieel om precies te bepalen in welke hoedanigheid een burgemeester waarschijnlijk een bestemming van persoonsgegevens is. Deze bepaling heeft niet alleen gevolgen voor de verantwoordelijkheid van de overheid die het initiatief neemt tot de mededeling (zie hierboven), maar ook voor haar bevoegdheden, voor haar hoedanigheid als verwerkingsverantwoordelijke⁸² en voor de mogelijkheid om gemeentediensten in te schakelen (met betrekking tot de beginselen van evenredigheid en minimalisering)⁸³.
71. Indien haar hoedanigheid van bestuurlijke politie bedoeld is om art. [Art. 133](#), lid 3 NLC toe te passen, is er reden om vraagtekens te plaatsen bij het gebrek aan onderscheid tussen haar rol en die van de andere administratieve overheden, d.w.z. de minister van Binnenlandse Zaken en de gouverneurs (en de minister-president). Als daarentegen het gezag van de burgemeester over de lokale politie in het geding is, moet worden verwezen naar de artikelen 42 en 45 van de WPI en naar het Politiecollege. Bovendien merkt de Autoriteit op dat het enige doel van de mededeling aan de burgemeester in zijn hoedanigheid van bestuurlijke politieautoriteit is "hem op de hoogte te houden van de opvolging". Deze formulering is echter onverenigbaar met het concept van "gebruiken" van gegevens als bedoeld in artikel 12 van het ontwerpbesluit.

⁸² Over deze kwestie, zie COC, advies uit eigen beweging van 11 februari 2021 met betrekking tot de vraag wie de verwerkingsverantwoordelijke is voor gegevensverwerkingen door de politiediensten in het kader van de uitvoering van politiebepaalde opdrachten enerzijds en voor gegevensverwerkingen onder de AVG anderzijds (https://www.controleorgaan.be/files/DD200026_Verwerkingsverantwoordelijke_GPI_N.PDF.)

⁸³ En of de omzendbrief van 1 december 2006 betreffende de vermindering en vereenvoudiging van bepaalde administratieve taken van de lokale politie al dan niet moet worden aangepast.

72. Met betrekking tot de bevoegdheid van de burgemeester omschreven in de nieuwe gemeentewet, moet worden verwezen naar «maatregelen van de bestuurlijke politie»⁸⁴.
73. De Autoriteit is ook verbaasd over het gebrek aan consistentie met de bepalingen inzake de bevoegdheid van de burgemeester om zaken te raadplegen (in de zin van artikel 458ter van het strafwetboek) in de LVIC-wet en de gemeenschapsdecreten⁸⁵. Indien nodig zal het ontwerp daarom worden aangepast om de doeleinden van de verwerking te specificeren met betrekking tot de wettelijke bevoegdheden⁸⁶ van de bestemming.

II.3. Het proportionaliteitsbeginsel en het beginsel van de minimale gegevensverwerking

74. Art. 2, 2° van het wetsontwerp tot wijziging van de WOG beoogt een nieuw lid in te voegen in art. 4 van de WOG⁸⁷, volgens hetwelk «bij de toepassing van *deze wet rekening wordt gehouden met een leidend beginsel van Verordening 2016/679, dat stelt dat de verwerking van persoonsgegevens gericht moet zijn op het dienen van de mensheid en dat het recht op bescherming van persoonsgegevens, dat geen absoluut recht is, moet worden beschouwd in verhouding tot de functie ervan in de samenleving en moet worden afgewogen tegen andere grondrechten, overeenkomstig het evenredigheidsbeginsel*»⁸⁸.

⁸⁴ Zie Mercuriale van PG I. de la Serna, La montée en puissance de la répression administrative : recul ou progrès d'une société, 2 septembre 2019, p. 6, ainsi que les références citées (https://www.ommp.be/sites/default/files/ui/mercuriale_2019_mo_0.pdf).

⁸⁵ Zie het Vlaams decreet van 21 mei 2021 houdende de machtiging van de Vlaamse deelnemers aan en de regeling van de modaliteiten van deelname aan LVIC-R.

⁸⁶ Voor zover de wetgever de intentie heeft om dit ontwerp aan te passen, moet ook rekening worden gehouden met het overleg per geval als bedoeld in artikel 35 van het voorontwerp van wet *betreffende de gemeentelijke bestuurlijke handhaving, de instelling van een gemeentelijk integriteitsonderzoek en houdende oprichting van een Directie Integriteitsbeoordeling voor Openbare Besturen, dat artikel 119ter van de nieuwe gemeentewet opnieuw invoert* en waarover de Autoriteit advies 245/2022 uitbracht op 21 oktober 2022 (<https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-245-2022.pdf>); zie ook advies 13/2022 van 18 november 2022 van het Federaal Instituut voor de bescherming en de bevordering van de Rechten van de mens (https://institutfederaaldroitshumains.be/sites/default/files/2022-11/Advies%20FIRM%20Gemeentelijke%20bestuurlijke%20handhaving_0.pdf).

⁸⁷ Reproductie van de 4de overweging van de AVG.

⁸⁸ Parl. St., Kamer, 2021-2022, DOC 55-2793/001, blz. 98; De Autoriteit wijst erop dat overweging 4 van de AVG (die in de bovenstaande bepaling is overgenomen) betrekking heeft op artikel 1 van de AVG, waarnaar in de overwegingen 1 tot en met 3, 9, 10 en 13 ook wordt verwezen. De derde paragraaf van artikel 1 heeft betrekking op *"het vrije verkeer van persoonsgegevens in de Unie noch beperkt noch verboden wordt om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens"*. Een gezamenlijke lezing van alle overwegingen die van toepassing zijn op artikel 3 maakt duidelijk dat het de bedoeling van de auteurs was om te voorkomen dat verschillen in het beschermingsniveau tussen de lidstaten *«het vrije verkeer van dergelijke gegevens in de hele Unie zouden belemmeren»*. De bepalingen van de AVG eerbiedigen "alle grondrechten" (overweging 4), maar staan de nationale wetgevers toe om de regels van de AVG te specificeren (overweging 10). Met andere woorden, de regels van de AVG bieden de minimale harmonisering die nodig is om het vrije verkeer van gegevens te waarborgen en, hoewel de AVG de nationale wetgevers toestaat om bepaalde verwerkingen strenger te reguleren, verhindert de hiërarchie van normen dat een nationale wetgever een regel aanneemt die afwijkt van de bepalingen van de AVG. Naar aanleiding van zijn arrest 110/25022 herinnerde het Grondwettelijk Hof aan het volgende *«het voorstel dat is voorafgegaan aan de aanneming van artikel 22 van de Grondwet beklemtoonde « de bescherming van de persoon, de erkenning van zijn identiteit en de belangrijkheid van zijn ontplooiing en die van zijn gezin » en het onderstreepte de noodzaak om het privéleven en het gezinsleven te beschermen tegen « inmenging, onder meer als gevolg van de onafgebroken ontwikkeling van de informatietechnieken, wanneer maatregelen van opsporing, onderzoek en controle door de overheid en particuliere instellingen worden uitgevoerd bij het uitoefenen van hun functie of hun activiteit » (Parl. St., Senaat,*

75. In zijn arrest 52/2021 oordeelde het Grondwettelijk Hof dat de doelstelling om terrorisme en radicalisering te bestrijden onbetwistbaar beantwoordt aan een dwingende maatschappelijke behoefte⁸⁹.
76. **De Autoriteit is het eens met deze vaststelling en zal nu onderzoeken of de in het ontwerp voorziene middelen noodzakelijk en evenredig zijn om in deze sociale behoefte te voorzien.** Zoals het Grondwettelijk Hof aangaf in zijn arrest 110/2022 «*De bescherming van het grondrecht op eerbiediging van het privéleven op het niveau van de Unie vereist, volgens vaste rechtspraak van het Hof van Justitie, dat de uitzonderingen op de bescherming van de persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven*»⁹⁰. *Bij de beoordeling van de evenredigheid van maatregelen met betrekking tot de verwerking van persoonsgegevens, dient rekening te worden gehouden met, onder meer, het geautomatiseerde karakter ervan, de gebruikte technieken, de accuraatheid, de pertinentie en het al dan niet buitensporige karakter van de gegevens die worden verwerkt, het al dan niet voorhanden zijn van maatregelen die de duur van de bewaring van de gegevens beperken, het al dan niet voorhanden zijn van een systeem van onafhankelijk toezicht dat toelaat na te gaan of de bewaring van de gegevens nog langer is vereist, het al dan niet voorhanden zijn van afdoende controlerechten en rechtsmiddelen voor de betrokkenen, het al dan niet voorhanden zijn van waarborgen ter voorkoming van stigmatisering van de personen van wie de gegevens worden verwerkt en het al dan niet voorhanden zijn van waarborgen ter voorkoming van foutief gebruik en misbruik van de verwerkte persoonsgegevens door de overheidsdiensten*⁹¹ »⁹².
77. De Autoriteit wijst erop dat de toename van het aantal betrokken diensten tot gevolg heeft (en zelfs tot doel heeft) dat er meer persoonsgegevens worden verwerkt en dat deze gegevens kunnen worden

B.Z. 1991-1992, nr. 100-4/2°, p. 3). In dat voorstel werd eveneens aangegeven dat de wetgever « *het recht op de eerbiediging van het privéleven en het gezinsleven op geen enkele wijze mag uithollen; anders schendt hij niet alleen een grondwetsregel, maar ook internationale rechtsregels* » (ibid.) » (Arrest van 22 september 2022, B.7.4. blz. 27-27 (<https://www.const-court.be/public/n/2022/2022-110n.pdf>)).

De voorwaarde van noodzakelijkheid en het evenredigheidsbeginsel zijn ook opgenomen in overweging 39 van de AVG, die betrekking heeft op art. 5.1.c van de AVG (zie in deze zin. HvJEU, 22 juni 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraaf 110 en de vermelde jurisprudentie en HvJEU, 11 december 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, EU:C:2019:1064, paragraaf 48).

⁸⁹ Arrest van 1 april 2022, B.13, blz. 29 (<https://www.const-court.be/public/n/2021/2021-052n.pdf>).

⁹⁰ HvJEU, 16 december 2008, C-73/07, *Satakunnan Markkinapörssi et Satamedia*, punt 56; 8 april 2014, C-293/12 en C-594/12, *Digital Rights Ireland e.a.*, punten 51 en 52; 6 oktober 2015, C-362/14, *Schrems*, punt 92, 21 december 2016, C-203/15 en C-698/15, *Tele2 Sverige en Watson e.a.*, punten 96 en 103, 6 oktober 2020, C-511/18, C-512/18 en C-520/18, *La Quadrature du Net e.a.*, punt 130.

⁹¹ Arrest nr. 108/2016 van 14 juli 2016, B.12.2; Arrest nr. 29/2018 van 15 maart 2018, B.14.4; Arrest nr. 27/2020 van 20 februari 2020, punt B.8.3; EHRM, grote kamer, 4 mei 2000, *Rotaru v. Roemenië*, § 59, beslissing 29 juni 2006, *Weber en Saravia v. Duitsland*, § 135; 28 april 2009, *K.H., e.a. vs. Slowakije*, §§ 60-69, grote kamer, 4 december 2008, *S. en Marper vs. Verenigd Koninkrijk*, § 101-103, 119, 122 en 124; 18 april 2013, *M.K. vs. Frankrijk*, § 37 en 42-44; 18 september 2014, *Brunet vs. Frankrijk*, § 35-37; 12 januari 2016, *Szabo en Vissy vs. Hongarije*, § 68; HvJEU, 8 april 2014, C-293/12, *Digital Rights Ireland e.a.*, en C-594/12, *Kärntner Landesregierung e.a.*, punten 56 en 66.

⁹² Arrest van 22 september 2022, B.22, blz. 57-58 (<https://www.const-court.be/public/n/2022/2022-110n.pdf>); De Autoriteit voegt eraan toe dat in het Hof van *Justitie in de zaak Asociația de Proprietari bloc M5A ScaraA*, heeft verduidelijkt dat de noodzakelijkheidsvoorwaarde moet worden onderzocht in samenhang met het beginsel van minimale gegevensverwerking, neergelegd in artikel 5, lid 1, punt c), van de AVG (*op. cit.*, §48); Zie ook HvJ-EU, 5 april 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, punt 52 en 11 december 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, EU:C:2019:1064, punt 57.

gecombineerd, waardoor de rechten en vrijheden van de betrokken personen meer worden aangetast⁹³⁹⁴.

78. Bovendien, voor zover de bepalingen met betrekking tot de GGB sinds 2016 zijn opgenomen in de WPA en sindsdien op grote schaal zijn bekritiseerd door de erkende doctrine⁹⁵, is het niet aanvaardbaar om deze bepalingen te reproduceren zonder in het commentaar bij het betrokken artikel een empirische beoordeling op te nemen van het effect van deze maatregelen⁹⁶ op de preventie van terrorisme en gewelddadig radicalisme en dus van de overeenstemming van de betrokken bepalingen met de voorwaarde van noodzakelijkheid en het evenredigheidsbeginsel. Zoals een recent rapport aan de Hoge Commissaris voor de Mensenrechten van de Verenigde Naties ons eraan herinnert, maken we ons zorgen over de bedreigingen die het monitoren vormt voor democratieën (vrije vertaling) : « *Staten slagen er te vaak niet in om de doeltreffendheid aan te tonen van de monitoringssystemen die ze implementeren* »⁹⁷.
79. De Autoriteit is daarom van mening dat de memorie van toelichting bij het ontwerp een rechtvaardiging moet bevatten van de noodzakelijke en evenredige aard van de deelname van elk van de nieuwe partners en van het behoud van elk van de diensten die momenteel deelnemen. Deze rechtvaardiging zal moeten aantonen (op basis van zo objectief mogelijke criteria⁹⁸) dat de toename van de inmenging

⁹³ Zowel degenen met toegang tot de GGB als degenen die deelnemen aan LTF-overleg.

⁹⁴ In die zin: zie Advies 1/15 (*EU-Canada PNR Agreement*) van 26 juli 2017, EU:C:2017:592, paragraaf 128.

⁹⁵ Zie met name G. Vermeulen en S. De Coensel, "Gemeenschappelijke gegevensbanken in de strijd tegen het terrorisme: noodzakelijke maar te brede sleepnetten," *POLITIE EN RECHT*, vol. 4, no. 4, blz. 164–177, 2021 (<http://hdl.handle.net/1854/LU-8733193>).

⁹⁶ Met name gebaseerd op misdaadstatistieken (politiestatistieken van 2000 tot en met het elfde kwartaal van 2022, kunnen worden geraadpleegd via de volgende link :

https://www.politie.be/statistieken/sites/statspol/files/statistics_files_upload/Criminaliteit%20C3%A9%20-%20Criminaliteit%20crimi_nl/01_Rapporten/01_Federaal/rapport_2022_trim3_nat_belgie_nl.pdf.

⁹⁷ Verslag van 4 augustus 2022, The right to privacy in the digital age, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement>, punt 54.

⁹⁸ De Autoriteit wijst erop dat de rechtvaardiging voor inmenging in het belang van de veiligheid wordt beoordeeld in het licht van de context die van kracht was op het moment dat de norm werd goedgekeurd. Bijgevolg moet de evaluatie of de uitbreiding van een maatregel noodzakelijk en evenredig is, vergezeld gaan van een verwijzing in de toelichting naar de context (het plegen van terroristische daden, het niveau van de dreiging, enz.) rond de oprichting van de GGB en de uitbreiding van de verwerking naar andere entiteiten (voor achtergrond, zie C. Debrulle, *Lutte anti-terroriste ou combat liberticide ? Évaluation en 2016*, JDJ n° 360 - december 2016, blz. 10 ev. (<https://www.liquedh.be/wp-content/uploads/2016/12/idi-b360-12.16%20article%20claud%20debrulle.pdf>); zie ook M. Moucheron, « Délit politique et terrorisme en Belgique : du noble au vil », *Cultures & Conflits* [En ligne], 61 | printemps 2006, online gezet op 17 mei 2006 (<https://journals.openedition.org/conflits/pdf/2038>); C. Thomas, « L'organisation fédérale de la lutte antiterroriste en Belgique », *Courrier hebdomadaire du CRISP*, 2020/18-19 (n°2463-2464), blz. 5-66 (<https://www.cairn.info/revue-courrier-hebdomadaire-du-crisp-2020-18-page-5.htm#re289no289>); W. VAN LAETHEM, Het Coördinatieorgaan voor de dreigingsanalyse: Een punctuele analyse, *Vigiles*, 2007/4 (<https://bib.kuleuven.be/rbib/collectie/archieven/vigiles/2007-4-109-127.pdf>); M. Van Hoey, De Belgische gecoördineerde analyse van de dreiging, van de actie en van de informatiestroom: van AGG over OCAD naar (de toekomst van) het 'Actieplan Radicalisme', *Panopticon*, Jaargang I Volume 41 » Issue 3., 30 mei 2020 (www.maklu-online.eu/nl/tijdschrift/panopticon/jaargang-i-volume-41/issue-3-mei-juni-2020/de-belgische-gecoördineerde-analyse-van-de-dreiging/pdf). Het Hof van Justitie oordeelt inderdaad als volgt « *de omstandigheid dat aan overheidsinstanties te weinig middelen worden toegekend, in geen geval een legitieme reden kan vormen die vermag te rechtvaardigen dat inbreuk wordt gemaakt op de door het Handvest gewaarborgde grondrechten* » (HvJEU, 1 augustus 2022, C 184/20, OT c. Vyriausioji tarnybinės etikos komisija, , § 89) Hieruit volgt dat idealiter ook moet worden aangetoond dat de beoogde maatregelen niet

als gevolg van de bepalingen van het ontwerp beantwoordt aan een noodzaak om de maatregelen ter bestrijding van terrorisme en radicalisering te versterken.

80. Hierbij wordt de evenredigheid van de gegevensmededeling aan de deelnemende diensten beoordeeld in verhouding tot de mogelijkheid om het beoogde doel te bereiken door de mededeling van bepaalde gegevens door een van de basisdiensten alleen (bijvoorbeeld in de vorm van een politierapport of een uittreksel uit de door OCAD uitgevoerde dreigingsanalyse).
81. Om te voorkomen dat België er in de toekomst van wordt beschuldigd de doeltreffendheid van de monitoringsystemen die het toepast, niet aan te tonen, acht de Autoriteit het aangewezen om (in artikel 4 van het ontwerp) te bepalen dat statistieken zullen worden opgesteld **met het oog op de publicatie van een evaluatieverslag** (op in het ontwerp vast te stellen tijdstippen, maar niet minder dan om de drie jaar) over de doeltreffendheid van de toegepaste verwerkingsmethodes en de autoriteiten die bij het wetsontwerp en het uitvoeringsbesluit betrokken zijn ten oversrtaan van de doeleinden waarvoor de gegevens in de GGB zijn opgeslagen.
82. Het aantonen van het noodzakelijke en proportionele karakter van de mededeling zal ook betrekking moeten hebben op de methoden van deze mededeling. Bij deze gelegenheid zal moeten worden aangetoond hoe de systematische en exclusieve centralisatie van gegevens op het niveau van de GGB eerder aan het beoogde doel beantwoordt dan de toegang die wordt gemoduleerd volgens de nagestreefde doeleinden volgens een kruispuntbankensysteem, dan een eenvoudige "pushbericht" aan andere belanghebbende diensten of een mededeling van informatie, gedaan door de directie van een dienst aan zijn betrokken tegenhanger(s) (ten minste voor de ernstigste gevallen)⁹⁹.

De zaak Conings en de verplichting voor de LTF om een lijst van maatregelen door te nemen die genomen kunnen worden (hoofdstuk 3 van het wetsontwerp)

83. Artikel 31 van het wetsontwerp bepaalt het volgende «*met het oog op de verrijking van persoonsgegevens en informatie over entiteiten en de opvolging en het nemen van maatregelen ten*

bedoeld zijn om een desinvestering in de politie- en veiligheidsdiensten te compenseren (zie voor achtergrondinformatie hierover het evaluatierapport over de hervorming van de politie, punt 4.1.11., blz. 40 e.v. <https://www.police.be/5998/sites/5998/files/downloads/cfp-adv-2009-05-29-f.pdf>); zie ook de rubriek "personeel" van het jaarverslag 2021 van de federale politie, waarin melding wordt gemaakt van de stabiliteit van het tekort aan operationeel personeel (<https://rapportannuel.policefederale.be/organisation/notre-personnel/>), terwijl het 3e verslag van de aanslagencommissie ook de aanbeveling bevat dat "de nodige inspanningen moeten worden geleverd om ervoor te zorgen dat alle diensten over voldoende middelen beschikken, met name na de verbreding van hun takenpakket...", op.cit. blz. 133).

⁹⁹ En om aan te tonen dat het ontwerp technologische oplossingen vereist om zich aan te passen aan de normen (waarbij de rechtsstaat wordt gerespecteerd) en, omgekeerd, geen vermijdbare inmenging veroorzaakt in de rechten en vrijheden van betrokkenen (bijvoorbeeld door de verantwoordelijkheid voor de verwerking te verminderen of door te voorzien in gegevensverstrekking die verder gaat dan wat noodzakelijk is) om zich aan te passen aan de werking van een bestaande technologische oplossing.

aanzien van de in de gemeenschappelijke gegevensbank T.E.R., gevalideerde entiteiten, worden er persoonsgegevens en informatie uit de gemeenschappelijke gegevensbank T.E.R., alsook andere persoonsgegevens en relevante informatie, waaronder geclassificeerde informatie (...) uitgewisseld binnen een of meer overlegplatformen die bij elk gerechtelijk arrondissement zijn opgericht, onder de naam 'Lokale task force' (hierna 'LTF') (...) ».

84. Zoals *supra*¹⁰⁰ aangegeven, functioneren de LTF's sedert lange tijd (buiten een wettelijk kader) en daarom wil het wetsontwerp :

- hen een wettelijke basis verschaffen¹⁰¹ ;
- hun specifiek doeleinde bepalen, namelijk het voeden van de GGB, toezicht houden en maatregelen nemen (art. 31) ;
- hun samenstelling uitbreiden naar VZ en voorzien in de mogelijkheid «*andere diensten, organen of instanties uitnodigen wegens de bijdrage die ze door hun functie of bevoegdheden kunnen leveren aan een gerichte en geïndividualiseerde opvolging van de entiteit*» (art. 32, §1) ;
- hun taken bepalen (met de bevoegdheid voor de Koning om ze uit te breiden)¹⁰² (art. 32, §2) ;
- voorzien in verplicht overleg over de gepastheid van het nemen of opheffen van maatregelen (niet-limitatief opgesomd in art. 33, §2)¹⁰³ bij validatie of «*wanneer nieuwe persoonsgegevens en informatie (...) tot een wijziging van maatregelen ten aanzien van de entiteit kunnen leiden, (...)*» (art. 33, §1, lid 2) ; en
- een "proactieve aanpak" ¹⁰⁴ implementeren (art. 33, §1 lid 3).

85. In het commentaar bij hoofdstuk 3 van het wetsontwerp¹⁰⁵ staat dat het doel van het wetsontwerp erin bestaat de uitwisseling en communicatie te bevorderen tussen de verschillende diensten die verantwoordelijk zijn voor terrorisme-extremisme en verder te optimaliseren, waarvan het belang door de zaak Conings werd herbevestigd. De Autoriteit gaat ervan uit dat de aanvrager, door uitdrukkelijk

¹⁰⁰ Bij het onderzoek van de doeleinden van LTF.

¹⁰¹ Onvoldoende met betrekking tot het legaliteitsbeginsel, zoals is aangetoond *supra*.

¹⁰² Machtiging die vatbaar is voor kritiek in het licht van het legaliteitsbeginsel (zie *supra*.)

¹⁰³ Het gaat "met name" om meldingen, maatregelen met betrekking tot de mogelijkheid om het beroep van privédetective uit te oefenen, intrekking van vergunningen, certificaten en veiligheidsattesten, maatregelen die onder de bevoegdheid vallen van de dienst sociale informatie en onderzoek van de FOD Werkgelegenheid (zoals een sociaal onderzoek), financiële onderzoeken door de CTIF, maatregelen die onder de bevoegdheid vallen van de RVA of zijn regionale tegenhangers, maatregelen met betrekking tot de toegang tot het grondgebied, verblijf, vestiging en verwijdering van vreemdelingen, weigering, intrekking of ongeldigverklaring van paspoorten of reis- of identiteitsdocumenten, verplichte inschrijving of schrapping uit bevolkingsregisters, bevrozing van tegoeden, toezicht door de politie of inlichtingendiensten en toezicht op de sociale media van de entiteit (waarvan het ontwerp niet specificeert welke overheid deze maatregel zal uitvoeren).

¹⁰⁴ Dit betekent dat de resultaten van het overleg moeten worden doorgegeven aan de bevoegde instanties die de nodige maatregelen moeten nemen.

¹⁰⁵ Die wil voorzien in de uitwisseling van gegevens over een entiteit, binnen een platform (de LTF) en dat de LTF overleg pleegt over de mogelijk te nemen maatregelen zodra een entiteit is gevalideerd in de GGB.

te verwijzen naar een recent tragisch geval, wil aantonen dat de grotere inmenging¹⁰⁶ waarin de voorgestelde bepalingen voorzien, daadwerkelijk zal voorkomen dat dergelijke gebeurtenissen zich opnieuw voordoen, dat het nagestreefde doel niet kan worden bereikt met een maatregel die minder ingrijpt in het recht op eerbiediging van het privéleven of in het recht op bescherming van persoonsgegevens, en dat er een evenwicht bestaat tussen de inmenging in het recht op eerbiediging van het privéleven en op bescherming van persoonsgegevens en het nagestreefde doel¹⁰⁷.

86. In de eerste plaats wijst de Autoriteit erop dat een beknopte beschrijving van de zaak en het leggen van een verband tussen deze zaak en het belang van de mededeling, waarvan slechts wordt vermeld dat zij opnieuw is bevestigd, niet kan worden beschouwd als een bewijs van de noodzakelijke en evenredige aard van de inmenging.
87. Om de aanvrager zo goed mogelijk te adviseren over de bewijzen die ter staving van deze bewering kunnen worden aangevoerd, heeft de Autoriteit echter het verslag geraadpleegd van de hoorzitting van generaal-majoor Philippe Boucké (sinds 18 september 2020 hoofd van de ADIV), in het kader van de zaak Jürgen Conings, voor de Commissie Defensie van De Kamer¹⁰⁸. De belangrijkste bevindingen waren dat de communicatiestromen waarvan werd vastgesteld dat ze versterkt moesten worden, betrekking hadden op de interne communicatie (de ADIV had te kampen met interne interpersoonlijke spanningen tot kort voor de incidenten)¹⁰⁹ en met bij naam genoemde partners«*(Veiligheid van de Staat, OCAD, FedPol)*»¹¹⁰. De behoefte om gegevens met andere partners te delen wordt dus in het hoorzittingsverslag met betrekking tot deze zaak niet genoemd of aangetoond.
88. Aan de andere kant maakt het verslag van de hoorzitting het mogelijk om de maatregelen te identificeren, die de gebeurtenissen die hebben plaatsgevonden, effectief kunnen voorkomen. Hij verklaarde met name dat de veiligheidsmachtiging in 2020 niet was verlengd, maar dat de verordening toegang tot wapens geen gevolgen verbond aan het verlies van een veiligheidsmachtiging¹¹¹ en dat als de ADIV niet in staat was een vertegenwoordiger naar de LTF te sturen op de dag dat het dreigingsniveau ten aanzien van de betrokkene door OCAD werd verhoogd, dit te wijten was aan (1) een gebrek aan personeel¹¹² en (2) de noodzaak om voorrang te geven aan een andere dreiging¹¹³,

¹⁰⁶ Als gevolg van de opname van actoren buiten de straf- en veiligheidsketen (met inbegrip van het VZ) bij de overheden die gegevens met betrekking tot entiteiten in het kader van LTF-overleg moeten meedelen en meegedeeld moeten krijgen.

¹⁰⁷ Daadwerkelijk beriekbaar.

¹⁰⁸ Parl.St. 23 september 2021, 55-2206/001, blz. ev.

¹⁰⁹ *Ibidem.*, blz. 12.

¹¹⁰ *Ibidem.*, blz. 14.

¹¹¹ « Pro memorie: een veiligheidsmachtiging verleent een lid van Defensie toegang tot geclassificeerde informatie indien hij die in het kader van zijn functie nodig heeft, of tot geclassificeerde zones. Het gaat hierbij hoegenaamd niet over het al dan niet toegang hebben tot wapens of tot munitiedepots », *Ibidem.*, blz. 10

¹¹² « Het lokaal detachement slechts over twee agenten beschikte in deze periode – intussen liet hij de ploeg versterken – en dat één van beiden in zwangerschapsverlof was. De enige aanwezige agent had die dag twee vergaderingen in zijn agenda en heeft om die reden niet deelgenomen aan de vergadering » *Ibidem.*, blz. 11. « De wet van 30 november 1998 baken de rollen, functies en taken van de inlichtingen- en veiligheidsdiensten af. De ADIV heeft een breed scala aan wettelijke opdrachten, die ruimer gaan dan die welke in de organieke wet worden geregeld. De lijst met verplichte opdrachten die de Dienst heeft opgesteld, telt 21 bladzijden », *Ibidem.*, blz. 13.

¹¹³ Als "hete hangijzers" omschreven, *Ibidem.*, blz. 14.

aangezien alle beschikbare bewijzen, met inbegrip van die van politie en justitie, erop wezen dat er op dat precieze moment weinig of geen bewijzen waren tegen Jürgen Conings¹¹⁴.

89. De Autoriteit concludeert dat de noodzaak en evenredigheid van de deelname van VZ aan de LTF niet is aangetoond bij de huidige stand van het ontwerp en niet lijkt te kunnen worden aangetoond op basis van de case die in de opmerkingen wordt aangehaald. Anderzijds blijkt uit het aangehaalde voorbeeld heel duidelijk de noodzaak om de diensten die verantwoordelijk zijn voor de toegang tot wapens¹¹⁵ (binnen de verschillende overheden waarvan de respectieve agenten in de uitoefening van hun functie toegang hebben tot wapens) in kennis te stellen van de intrekking van een veiligheidsmachtiging van een van hun agenten, maar vooral van het negatieve resultaat van een rapport na een psychologisch onderzoek waaraan deze categorie agenten vermoedelijk periodiek wordt onderworpen.
90. De noodzaak en evenredigheid van het uitstellen van het nemen van een maatregel door deze te onderwerpen aan voorafgaand overleg (zie bijvoorbeeld art. 33, §2, 4° van het wetsontwerp m.b.t. het intrekken van een veiligheidsmachtiging) en dus van de wederzijdse mededeling van gegevens tussen diensten, die elk hun eigen bevoegdheden ter zake hebben, wordt in de huidige staat van het ontwerp evenmin aangetoond. Er moet dus een onderscheid worden gemaakt tussen verplicht voorafgaand overleg (dat zeker gerechtvaardigd is ten aanzien van het parket) en de mededeling in real time of a posteriori van informatie met betrekking tot het nemen van een maatregel, met de diensten die over gegevens over de betrokkene beschikken.
91. Bovendien moeten de uit te nodigen diensten (die gegevens moeten door te geven of verzamelen door deel te nemen aan LTF) op zijn minst identificeerbaar zijn. Het commentaar bij artikel 32 verwijst in dit verband naar "*hun bevoegdheden of functies*" en naar hun "*betrouwbare*" aard. Deze elementen zijn niet van dien aard dat een betrokkene zich ervan kan vergewissen dat de verwerking van zijn of haar gegevens door deze uitgenodigde dienst noodzakelijk is en in verhouding staat tot het beoogde doel. De criteria staan nader omschreven in het commentaar bij artikel 32. Voor diensten die geen deel uitmaken van de strafrechtelijke en veiligheidsketen of ten aanzien waarvan de deelneming beperkt is tot de verstrekking van informatie die noodzakelijk is om een maatregel te kunnen nemen, dient in ieder geval te worden bepaald dat de betrokkene reeds "*bekend*" moet zijn bij de deelnemende dienst en dat deze dienst over informatie moet beschikken die voor hem "*nuttig*" kan zijn.
92. Wanneer artikel 31 van het wetsontwerp¹¹⁶ wordt geherformuleerd, moet het **begrip van "uitwisseling" van gegevens ook worden verduidelijkt**. Strikt genomen komt dit niet overeen met het verwerken van gegevens en het is daarom niet mogelijk om hieruit de voorwaarden voor gegevensverwerking af te leiden. Er zal vooral op worden gelet dat het noodzakelijke en

¹¹⁴ In 2019, «Overigens heeft Defensie datzelfde jaar nog gereageerd door een klacht in te dienen bij de politie. Het parket heeft het dossier geseponneerd», *Ibidem*, blz. 9 en 11.

¹¹⁵ Om de toegang tot wapens en munitie voor de betrokken persoon te verbieden.

¹¹⁶ Wat betreft de noodzaak van herformulering in het licht van het beginsel van doelbinding, zie hierboven.

evenredige karakter van de "wederkerigheid" die het begrip uitwisseling aan de mededeling van gegevens verbindt, wordt aangetoond. Met andere woorden, voor elk van de potentiële deelnemers en genodigden en voor elke gegevenscategorie zal worden aangetoond (in het commentaar bij hoofdstuk 3) dat de mededeling van gegevens¹¹⁷ (die de deelnemer nog niet heeft verzameld krachtens zijn eigen opdrachten) inderdaad noodzakelijk en evenredig is. Op basis van dit bewijs zou het bijvoorbeeld mogelijk moeten zijn om vast te stellen (1) wat de criteria zijn om te oordelen dat een maatregel tot ongeldigverklaring van een paspoort "*in onderling overleg*" moet worden genomen (en niet eenzijdig door de bevoegde overheid), (2) welke overheden gerechtvaardigd zijn om deel te nemen aan (of te worden uitgenodigd om deel te nemen aan) een dergelijk overleg (in plaats van het resultaat van het overleg te ontvangen als zij de bevoegde overheid zijn om de maatregel te nemen), en (3) of Consulaire Zaken (en/of andere buitenlandse deelnemers aan de strafrechtelijke en veiligheidsketen) alleen moeten worden uitgenodigd om hun gegevens over de besproken entiteit te delen (of dat het voor hen haalbaar is om een maatregel te nemen¹¹⁸) of dat zij ook op de hoogte moeten worden gebracht van de gegevens van de andere overheden in de strafrechtelijke en veiligheidsketen¹¹⁹ ?

Categorieën verwerkte gegevens

93. Het wetsontwerp voorziet in de verwerking van de persoonsgegevens opgesomd in art. 6, §2. Door een opsomming te geven van de gegevens die waarschijnlijk zullen worden verwerkt "*in de gegevensbank*", maakt het ontwerp het echter niet mogelijk om te begrijpen welke van deze gegevens waarschijnlijk door welke dienst zullen worden verwerkt (en nog minder om te beoordelen of ze noodzakelijk en evenredig zijn).
94. Zoals hierboven vermeld¹²⁰, is het echter noch noodzakelijk, noch evenredig dat de Dienst Erediensten en Vrijzinnigheid te weten komt of een niet-religieuze EPV ingeschreven is bij de GGB. Evenzo zou de Thesaurie, zoals het ontwerp er nu uitziet, niet de gezondheidsgegevens mogen raadplegen van een entiteit waarvan de tegoeden worden bevroren, zouden gevangenen niet de gegevens mogen verwerken van personen die niet van hun vrijheid zijn beroofd en zou de Dienst Vreemdelingenzaken niet betrokken mogen worden bij de verwerking van entiteiten die alleen de Belgische nationaliteit hebben.
95. Bijgevolg is de Autoriteit van mening dat artikel 6 moet worden geherformuleerd om - voor elk van de partnerdiensten - een onderscheid te maken tussen de categorieën gegevens waarover deze diensten

¹¹⁷ Maar ook de aanwezigheid van elk van deze deelnemers aan de LTF.

¹¹⁸ Bijvoorbeeld de annulering van een reisdocument.

¹¹⁹ De Autoriteit is van mening dat, gezien de huidige stand van het elementenl waarover zij beschikt, deze tweede mogelijkheid moet worden uitgesloten.

¹²⁰ Bij de analyse van de doeleinden.

beschikken en die zij in het kader van dit ontwerp mogen meedelen "in naleving van de behoefte om te kennen" van aan de andere diensten (met name de deelnemende diensten), en de gegevens die door andere deelnemers aan een overlegvergadering worden meegedeeld en waarvan de andere deelnemende diensten kennis kunnen nemen. Bij deze gelegenheid zal moeten worden aangetoond dat het ontwerp vereist dat de technologische toepassingen worden aangepast aan de normen (met inachtneming van de rechtsstaat) en niet omgekeerd, dat het een vermijdbare aantasting van de rechten en vrijheden van de betrokkenen¹²¹ veroorzaakt met het oog op de aanpassing aan de werking van een bestaande technologische toepassing.

96. De Autoriteit wijst er ook op dat in het geval van gegevens die, ten minste gedeeltelijk, door andere diensten worden bijgehouden, het beginsel van de minimale gegevensverwerking vereist dat wanneer het doel kan worden bereikt door gegevens van één dienst door te geven (bijvoorbeeld een uittreksel uit de dreigingsanalyse van OCAD of een verslag van de lokale politie), dit op die manier moet gebeuren.
97. Wat de **gegevenscategorieën** zelf betreft, merkt de Autoriteit op dat het commentaar bij artikel 6 weliswaar een vrij goed inzicht geeft in de gegevens die waarschijnlijk zullen worden verwerkt, maar wijst zij erop dat, zoals hierboven aangegeven, voor zover de wet tot oprichting van de GGB dateert van 2016, het niet toelaatbaar is de bepalingen ervan over te nemen zonder in het commentaar bij het betrokken artikel een empirische beoordeling op te nemen van de vraag of de betrokken bepaling voldoet aan de voorwaarde van het noodzakelijkheid- en evenredigheidsbeginsel. Bijgevolg moet, met betrekking tot de categorieën gegevens die worden verwerkt, op basis van feitelijke en objectieve elementen worden aangetoond dat de voorgestelde verwerking van persoonsgegevens doeltreffend is voor het bereiken van het beoogde doel, en dat de voordelen die voortvloeien uit de gegevensverwerking in kwestie dus groter zijn dan de nadelen die eruit voortvloeien voor de betrokkenen.
98. Zoals het geval is telkens wanneer het waarschijnlijk is dat gegevens uit politiedatabanken zullen worden verwerkt, benadrukt de Autoriteit dat de verantwoordelijken voor de verwerking moet worden gevraagd er in het bijzonder op toe te zien dat de gegevens die zij verwerken nauwkeurig en actueel zijn, overeenkomstig artikel 5.1.d) van de AVG. De feiten in kwestie kunnen worden betwist omdat ze niet noodzakelijk (definitief) worden vastgesteld. Bijgevolg is de Autoriteit van mening dat moet worden bepaald dat dergelijke gegevens alleen mogen worden verwerkt, ten minste door de partnerdiensten, als de precieze aard ervan is vastgesteld door middel van een "*retourstroom justitie*" (naar het model van die in artikel 646 van het Wetboek van Strafvordering¹²²).

¹²¹ Bijvoorbeeld door de verantwoordelijkheid voor de verwerking te vervagen of door te voorzien in de openbaarmaking van meer gegevens dan nodig is.

¹²² De categorieën van inlichtingen uit in kracht van gewijsde gegane beslissingen van een strafrecht, een hof van assisen of een hof van beroep, en die de in de algemene nationale gegevensbank, bedoeld in artikel 44/7 van de wet op het politieambt van 5 augustus 1992, hierna A.N.G. genoemd, opgenomen gegevens kunnen wijzigen, worden binnen dertig dagen aan de politie meegedeeld, op de door de Koning vastgestelde wijze, bij een in de Ministerraad overlegd besluit.

99. Met betrekking tot de verwerking (met name via onderlinge koppeling) van gegevens uit het strafregister van de betrokken personen moet - met het oog op de naleving van het evenredigheidsbeginsel - worden gepreciseerd dat minder ernstige veroordelingen, andere dan terroristische misdrijven die onder titel I ter van Boek II van het Strafwetboek vallen, of zelfs zeer oude¹²³ veroordelingen niet mogen worden verwerkt, althans niet door de partnerdiensten.
100. Aangaande het begrip "*gezondheidsgegevens*", benadrukt de Autoriteit dat het feit om de bepalingen in verband met de GGB uit de WPA te halen ertoe kan leiden dat wordt vergeten dat de politiediensten *«gegevens betreffende gezondheid (...)(enkel mogen verwerken) met het oog op het begrijpen van de omstandigheden waarin de betrokken persoon zich bevindt, evenals het garanderen van de veiligheid en het beschermen van de gezondheid van elke persoon die mogelijks in contact zou komen met de betrokken personen in het raam van politionele interventie. Wanneer gezondheidsgegevens worden verwerkt, wordt vermeld of deze gegevens al dan niet afkomstig zijn van beroepsbeoefenaren in de gezondheidszorg »*¹²⁴. Het zou moeilijk te rechtvaardigen zijn om andere diensten gezondheidsgegevens te laten verwerken. Deze bepaling moet daarom in het ontwerp worden opgenomen. De Autoriteit is ook van mening dat er in de toelichting bij artikel 6 op moet worden gewezen dat de verwerking van gegevens met betrekking tot de gezondheid niet hetzelfde is als de mededeling van een medisch dossier, waarop de artikelen 9 en 10 van de wet van 22 augustus 2002 betreffende de rechten van de patiënt¹²⁵ van toepassing blijven.
101. Het noodzakelijke en evenredige karakter van de verwerking van gegevens betreffende politieke opvattingen en religieuze of levensbeschouwelijke overtuiging door elk van de diensten die daarvan kennis kunnen nemen, zal ook moeten worden aangetoond in het commentaar bij artikel 6. Dit moet leiden tot uitsluiting van de verwerking van gegevens in verband met deze veroordelingen wanneer ze duidelijk niet nodig zijn voor het algemene doel van het ontwerp of voor de opdrachten van de diensten die toegang kunnen krijgen tot de GGB of kunnen worden uitgenodigd om deel te nemen aan een LTF. Het bovengenoemde bewijs zal het ook mogelijk maken **om te bepalen** of levensbeschouwelijke overtuigingen (ten onrechte) worden vermeld omdat ze in tal van bepalingen (waaronder art. 9.1. van de AVG) gezamenlijk worden vermeld **of dat bepaalde levensbeschouwelijke overtuigingen**

De categorieën van inlichtingen uit de beslissingen tot buitenvervolginstelling van onderzoeksrechtbanken, die de in de A.N.G. opgenomen gegevens kunnen wijzigen, worden binnen dertig dagen aan de politie meegedeeld, op de door de Koning vastgestelde wijze, bij een in de Ministerraad overlegd besluit.

De categorieën van inlichtingen uit door het openbaar ministerie genomen beslissingen tot seponering wegens onvoldoende bewijsmateriaal of geen overtreding, die de in de A.N.G. opgenomen gegevens kunnen wijzigen, worden binnen dertig dagen aan de politie meegedeeld, op de door de Koning vastgestelde wijze, bij een in de Ministerraad overlegd besluit.

¹²³ Zie over deze kwestie V. De Greef, « *Surveiller et punir... Les personnes condamnées par le casier judiciaire* », Le casier judiciaire. Approches critiques et perspectives comparées, onder leiding van V. De Greef en J. Pieret, Brussel, Larcier, coll. Crimen, 2011, blz. 21-39.

¹²⁴ Zie artikel 44/1, §3, 2° WPA, ingevoegd bij wet van 22 mei 2019. Diezelfde bepaling bepaalt bovendien « *de verwerking van gezondheidsgegevens waarnaar in dit artikel wordt verwezen, heeft nooit als gevolg de betrokkenen te laten onderwerpen aan medische onderzoeken* ».

¹²⁵ BS 26.09.2002.

daadwerkelijk aanleiding geven tot vrees voor gewelddadige radicalisering. In het eerste geval moeten deze gegevens natuurlijk uit het ontwerp worden weggelaten.

102. In het algemeen betekent naleving van de "*behoefte om te kennen*" van de deelnemende overheden dat het ontwerp een beschrijving moet bevatten van de technische en organisatorische maatregelen die moeten worden genomen (indien nodig door middel van een machtiging aan de regering) om ervoor te zorgen dat gegevens die door de bevoegde dienst worden doorgegeven voor een doel dat verband houdt met de preventie van terrorisme, niet voor andere doeleinden kunnen worden verwerkt door andere overheden.

Categorieën van gegevens verwerkt door "*andere bestemmingen*".

103. De Autoriteit verzoekt de aanvrager ook om in het commentaar bij artikel 24 te verduidelijken dat het er geenszins om gaat de "*andere bestemmingen*" van de informatiekaart toe te staan van deze bepaling gebruik te maken om "*onderzoek*" te doen (d.w.z. om de categorieën persoonsgegevens die zij mogen verzamelen, uit te breiden), noch om de gegevens die zij over de "*entiteiten*" hebben, te consolideren dankzij informatie die door de andere deelnemers is verstrekt, maar die voor hun eigen doeleinden irrelevant zou zijn. Om opnieuw het voorbeeld te nemen van de opmerking over de schooldirecteur die informatie kreeg om te voorkomen dat een jonge vroegtijdige schoolverlater naar een jihadistisch conflictgebied zou vertrekken, kan er geen sprake van zijn dat deze schooldirecteur gegevens over politieke veroordelingen, politiegegevens of enige andere categorie gegevens over leerlingen die zijn school bezoeken, zou mogen vastleggen die niet noodzakelijk zijn om de doelen te bereiken die zijn vastgelegd in de normen voor de organisatie van het onderwijs in de betreffende gemeenschap. Gezien het risico van misbruik verzoekt de Autoriteit de aanvrager te overwegen deze mogelijkheid van het meedelen van informatiekaart via de LVIC te illustreren en in het commentaar te verwijzen naar het relevante rechtskader.

Betrokken personen

104. De Autoriteit verwijst naar haar eerdere adviezen ter zake, naar het COC en het Comité I voor wat betreft de beoordeling van het noodzakelijke en evenredige karakter van de verwerking van de persoonsgegevens van de "*entiteiten*" die onder het ontwerp vallen. De Autoriteit is echter van mening dat de noodzaak en evenredigheid van de verwerking van de persoonsgegevens van deze entiteiten per dienst moet worden aangetoond.

Bijzonder geval "de minderjarige kinderen van entiteiten"

105. Artikel 3 van het ontwerp van koninklijk besluit geeft uitvoering aan artikel 6, § 2, eerste lid, 1°, 1), b) van het wetsontwerp en voorziet in de registratie van de identificatiegegevens van biologische of geadopteerde kinderen van een FTF die naar een jihadistisch conflictgebied zijn gereisd of die op weg

zijn naar België of die naar België zijn teruggekeerd na naar een jihadistisch conflictgebied te zijn gereisd, die in de GGB zijn geregistreerd en **tussen 0 en 18 jaar oud zijn**. Het verslag aan de Koning verduidelijkt dat het doeleinde van deze registratie erin bestaat «een overzicht te waarborgen van de kinderen die in een jihadistisch strijdgebied verblijven of hebben verbleven, teneinde voor de nodige opvolging te zorgen wanneer die kinderen naar België zouden terugkeren»¹²⁶ en «doordat hun identiteit bekend is, zal het ook mogelijk zijn om hen op te volgen zodra ze in ons land terug zijn na hun verblijf in een jihadistische conflictzone»¹²⁷. De Autoriteit is van mening dat de verwerking van de persoonsgegevens van deze minderjarigen - waarvan zij niet ontkent dat deze van belang is voor doeleinden die verband houden met de opdrachten van de inlichtingendiensten - veel verder gaat dan de doeleinden van registratie in een gegevensbank die toegankelijk is voor diensten waarvan de opdrachten geen verband houden met deze doeleinden. Deze "voor het geval dat"-verwerking van gegevens over kinderen van entiteiten - die niet moet worden verward met de situatie waarin de minderjarige zelf een entiteit is¹²⁸ - kan daarom niet worden uitgevoerd door geen enkele van de diensten die onder de bevoegdheid van de Autoriteit vallen.

106. De Autoriteit wil er terloops op wijzen dat het bestaan van een gegevensbank niet impliceert dat alle communicatie tussen twee diensten waarop de GGB betrekking heeft, noodzakelijkerwijs van dit kanaal gebruik moet maken. Zo kunnen bij melding van een geplande reis aan de Vreemdelingendienst of Consulaire Zaken of bij identificatie van een van deze minderjarigen aan een grenspost, de inlichtingendiensten worden geraadpleegd (en eventueel een negatief advies worden uitgebracht) zonder dat voornoemde diensten verplicht zijn de gegevens van de ouders van de betrokkene te raadplegen. Gezien de rechtvaardiging voor sommige van de voorgestelde bepalingen, zou een andersluidend besluit er waarschijnlijk toe leiden dat dit soort persoonsgegevens zelfs aan gezondheidswerkers of schoolhoofden wordt meegedeeld¹²⁹.

II.4. Verwerkingsverantwoordelijken

107. Betreffende de aanwijzing van de verwerkingsverantwoordelijken herinnert de Autoriteit aan haar vaste adviespraktijk **dat een overheidsinstantie in beginsel verantwoordelijk is voor de verwerking van gegevens die noodzakelijk is voor de vervulling van de haar**

¹²⁶ Verder zegt het Verslag aan de Koning «De meesten van hen zijn lokaal geboren, in de jihadistische conflictzone, en bestaan dus officieel niet. Hun registratie in de gemeenschappelijke gegevensbank T.E.R. is de enige manier om kennis te hebben van hun bestaan aangezien ze niet in het rijksregister zijn ingeschreven.»

¹²⁷ « Die kinderen zouden dus eventueel aan bod kunnen komen in de LIVC-R en de sociopreventieve diensten zouden indien nodig een begeleiding kunnen opstarten. Die kinderen worden daadwerkelijk beschouwd als kwetsbare personen, slachtoffers voor wie per geval in een specifieke opvolging moet worden voorzien. Zij worden niet besproken in de LTF tenzij er zich in de loop der jaren een problematische radicalisering voordoet ».

¹²⁸ Art. 6, § 1, van het wetsontwerp.

¹²⁹ Zie voor een voorbeeld van een geval waarin plaatsing op een lijst het risico op arrestatie vergroot, Saunders, J., Hunt, P. & Hollywood, J.S. Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot. *J Exp Criminol* 12, 347–371 (2016). <https://doi.org/10.1007/s11292-016-9272-0>

toevertrouwde openbare opdracht of die krachtens de betrokken wetgeving binnen de werkingssfeer van het aan haar toevertrouwde openbaar gezag valt¹³⁰.

108. Dit betekent dat heel duidelijk moet worden gemaakt aan welke overheid/overheden de GGB rapporteert (of bij welke overheid/overheden de GGB is opgericht¹³¹) en waarom. Een goed geformuleerde bepaling in dit verband moet het mogelijk maken om te bepalen:

- of de GGB "*gemeenschappelijk*" is voor de basisdiensten of voor de basisdiensten EN voor de partnerdiensten of voor de deelnemende diensten (van rechtswege of op uitnodiging ?) aan de LTF;
- Wie zijn de aangestelden¹³² van de verwerkingsverantwoordelijken (is het alleen OCAD)¹³³, en de beheerder van de GGB (de federale politie)¹³⁴ et de basisdiensten (maar hoe zit het met de ADIV, die een van de "inlichtingen- en veiligheidsdiensten" is waarnaar in de wet van 30 november 1998 wordt verwezen, maar die onder de bevoegdheid van de minister van Defensie valt)?¹³⁵ ?) ;
- dat de taken van de betrokken afdelingen verenigbaar zijn met de doelstellingen van de GGB ;

¹³⁰ Zie met name: advies nr. 129/2022 van 1 juli 2022 *betreffende de artikelen 2 en 7 tot en met 47 van een ontwerp van wet houdende diverse bepalingen inzake Economie*, overweging nr. 42 e.v.; advies 131/2022 van 1 juli 2022 *met betrekking tot een wetsontwerp tot oprichting van de Kunstwerkcommissie en ter verbetering van de sociale bescherming van de kunstwerkers*, overwegingen 55 en volgende; advies nr. 112/2022 van 3 juni 2022 *met betrekking tot een ontwerp van wet tot wijziging van het Sociaal Strafwetboek met het oog op de invoering van het eDossier-platform*, overwegingen nrs. 3-41 en 87-88; advies nr. 231/2021 van 3 december 2021 *met betrekking tot een voorontwerp van ordonnantie betreffende de interoperabiliteit van elektronische tolheffingssystemen voor het wegverkeer*, overwegingen nrs. 35-37; advies nr. 37/2022 van 16 februari 2022 *"concernant un avant-projet de décret instituant la plateforme informatisée centralisée d'échange de données 'E-Paysage'"* (niet beschikbaar in het Nederlands), overweging nr. 22; advies nr. 13/2022 van 21 januari 2022 *met betrekking tot een ontwerp van besluit van de Brusselse Hoofdstedelijke Regering betreffende de toekenning van premies voor de verbetering van het woonmilieu en een ontwerp van besluit van de Brusselse Hoofdstedelijke Regering tot wijziging van het besluit van de Brusselse Hoofdstedelijke Regering van 9 februari 2012 betreffende de toekenning van financiële steun voor energie*; overwegingen nrs. 9-17; advies nr. 65/2019 van 27 februari 2019 *betreffende een ontwerp van samenwerkingsakkoord tot wijziging van het samenwerkingsakkoord van 23 mei 2013 tussen het Waalse Gewest en de Franse Gemeenschap over het opstarten van een gemeenschappelijk initiatief om gegevens te delen en over het gemeenschappelijk beheer van dit initiatief*, overwegingen nrs. 90-113.

¹³¹ In dit verband is de overgang van «*kunnen de ministers van Binnenlandse Zaken en van Justitie gezamenlijk gemeenschappelijke gegevensbanken oprichten waarvan zij de verantwoordelijken voor de verwerking worden*» (Art.44/11/3bis §1, WPA) naar «*er wordt een gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" gecreëerd die de gemeenschappelijke verwerking mogelijk maakt, door alle of een deel van de basisdiensten en de partnerdiensten, van de persoonsgegevens en informatie betreffende de opdrachten inzake de voorkoming en de opvolging van terrorisme en extremisme, dat kan leiden tot terrorisme (...)*» waarvoor OCAD is aangewezen als verwerkingsverantwoordelijke (art.3 van het wetsontwerp en art. 5 van het ontwerp van KB) is een problematische regressie. Vergelijk: Art. 8, §4 van de wet van 16 oktober 2022 *ot oprichting van het Centraal register voor de beslissingen van de rechterlijke orde en betreffende de bekendmaking van de vonnissen en tot wijziging van de assisenprocedure betreffende de wraking van de gezworenen* (MB 24.10.2022).

¹³² In tegenstelling tot "gebruikers", die zich moeten houden aan de instructies voor toegang en gebruik die zijn vastgesteld door de verwerkingsverantwoordelijken, maar die niet onder hun gezag staan (in geval van onrechtmatige verwerking zullen zij dus waarschijnlijk hun eigen aansprakelijkheid oplopen, zowel jegens de betrokkenen als jegens de verwerkingsverantwoordelijken, maar NIET rechtstreeks de aansprakelijkheid van de verwerkingsverantwoordelijke jegens de betrokkenen)..

¹³³ Die effectief onder de gezamenlijke bevoegdheid van de ministers van Binnenlandse Zaken en Justitie wordt geplaatst (art. 5 van de wet van 10 juli 2006 betreffende de analyse van de dreiging (B.S. 20.07.2006)).

¹³⁴ Beide vallen onder de gezamenlijke bevoegdheid van de ministers van Binnenlandse Zaken en Justitie (Ibidem en art. 5 WPA).

¹³⁵ Art. 10, §2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (BS 18.02.1998).

- of een wijziging in de bevoegdheden van de auteur van de norm waarschijnlijk gevolgen zal hebben voor de verwerking van persoonsgegevens¹³⁶, en
- welke titel van de WVG¹³⁷ van toepassing is op de verwerking van persoonsgegevens die wordt uitgevoerd onder de verantwoordelijkheid van de verwerkingsverantwoordelijken van de GGB.

109. Wat deze laatste alinea betreft, worden de toepasselijke normen zowel bepaald door de betrokken bevoegde overheid als door het doel van de verwerking. Bij gebrek aan een bepaling die «*het verzamelen van gegevens bij de partnerdiensten door de operationele verwerkingsverantwoordelijke*»¹³⁸, voorschrijft, moet echter worden aangenomen dat de partnerdiensten gegevens doorgeven aan de verwerkingsverantwoordelijken van GGB¹³⁹. De AVG is daarom volledig van toepassing op deze mededeling door de partnerdiensten¹⁴⁰ die niet binnen de reikwijdte van de Richtlijn Politie-justitie vallen. Artikel 30, §2 van het ontwerp bevestigt deze interpretatie. De AVG is ook van toepassing op de toegang¹⁴¹ van deze zelfde partnerdiensten tot de GGB gegevens. Zodra deze gegevens zijn meegedeeld¹⁴², bepaalt artikel 30, §1, dat de verantwoordelijke voor de verwerking "die eigen is aan elke dienst" die de GGB voedt "verantwoordelijk blijft voor de kwaliteit van de gegevens", maar dat de verantwoordelijken voor de verwerking van de GGB-gegevens verantwoordelijk zijn voor de kwaliteit van de persoonsgegevens "die op de inlichtingenfiches zijn gevalideerd". Volgens de Autoriteit is deze formulering problematisch, aangezien het erop neer komt dat verwerkingsverantwoordelijken van de GGB worden vrijgepleit voor het verwerken (bv. meedelen aan derden) van onnauwkeurige gegevens, terwijl naleving van het nauwkeurigheidsbeginsel een voorwaarde is voor de rechtmatigheid van de verwerking, die in voorkomend geval inhoudt dat wordt afgezien van het verwerken (en vooral meedelen) van bepaalde

¹³⁶ Concreet, in geval van (1) de oprichting van een nieuwe gefedereerde dienst met bevoegdheden inzake vaststelling en vervolging van misdrijven die door de gefedereerde entiteit in kwestie worden vastgesteld of (2) de regionalisering (of communautarisering) van een dienst en zijn bevoegdheden, zal men moeten kunnen bepalen of de factor die de verwerking met zich meebrengt (feiten gepleegd in de entiteit, vermoedelijke dader gedomicilieerd in de entiteit, ...) verenigbaar is met de bevoegdheid van de wetgever die de essentiële elementen van de verwerking heeft bepaald. Gegevens die werden verzameld en geregistreerd tijdens de periode waarin de federale wetgever bevoegd was, mogen enkel in het tweede geval door een gewestelijke of gemeenschapsoverheid worden verwerkt, maar enkel gegevens die een band hebben met de gefedereerde entiteit; Opgemerkt moet worden dat de Autoriteit zich gewoonlijk onthoudt van commentaar op een toekomstige situatie waarvoor geen aanwijzing bestaat dat deze zich zal voordoen. Gezien de omvang van de inmenging in de rechten en vrijheden van de betrokkenen is de Autoriteit echter van mening dat, zodra met dit risico rekening kan worden gehouden, niet kan worden aanvaard dat de "nationale veiligheid" geldig kan worden ingeroepen voor een verwerking die onrechtmatig is geworden (in de zin van artikel 5.1.a) van de AVG) op grond van het feit dat de regionale of communautaire ad hoc-normen (en/of een samenwerkingsakkoord) niet konden worden vastgesteld vóór de daadwerkelijke tenuitvoerlegging van een staatshervorming.

¹³⁷ Met andere woorden, welke verwerkingen vallen onder respectievelijk de AVG, de Richtlijn Politiejustitie of Titel III en Verdrag 108 van de Raad van Europa?

¹³⁸ Ter herinnering: het ontwerp voorziet in de afschaffing van het begrip "verzameling" ten voordele van het begrip "opname van gegevens" om de IT-reëliteit weer te geven.

¹³⁹ Er zal echter aandacht worden besteed aan de opmerkingen die in dit hoofdstuk zijn gemaakt over de geschiktheid van het toepassen van het concept van verwerkingsverantwoordelijke van een gegevensbank.

¹⁴⁰ Zoals bijvoorbeeld Vreemdelingenzaken.

¹⁴¹ Of het nu gaat om toegang door lezen of door directe bevraging.

¹⁴² Namelijk na de GGB te hebben "gevoed".

gegevens. Deze valkuil komt voort uit het feit dat gegevensbeschermingsnormen vereisen dat er een verantwoordelijke voor de verwerking wordt aangewezen voor "*de verwerkingen*" (en niet alleen voor de gegevensbank)¹⁴³. **Het is daarom noodzakelijk om in het ontwerp te bepalen wie de verantwoordelijken voor de gegevensverwerking zijn, op basis van de verschillende verwerkingen die waarschijnlijk zullen worden uitgevoerd en niet op basis van de gegevensbank.**

110. Ten tweede, als het doel van de LTF is om de GGB te voeden¹⁴⁴ verzoekt de Autoriteit de aanvrager, in het belang van de voorspelbaarheid, om de redenen voor het gebrek aan afstemming tussen basis/GGB-partners en ambtshalve of uitgenodigde deelnemers aan de coördinatie van LTF¹⁴⁵ in detail toe te lichten in de Memorie van Toelichting.

111. Met betrekking tot de in artikel 28 bedoelde mededeling is de Autoriteit van mening dat het nodig is om in de toelichting te specificeren welke autoriteit onder de wettelijke verplichtingen (of de Verdragen) valt voor de mededeling van de gegevens in de GGB. In het geval van de verschillende diensten die verantwoordelijk zijn voor het verzamelen van de gegevens, elk voor hun eigen gegevens, zou de mogelijkheid om internationale doorgiften van gegevens in de GGB uit te voeren, helemaal achterwege kunnen worden gelaten (of, als dat niet mogelijk is, zou dat naar behoren moeten worden gemotiveerd). Als het daarentegen de operationeel beheerder is op wie deze mededelingsplicht rust, moet worden nagegaan of de verbintenis van OCAD om door andere diensten meegedeelde gegevens¹⁴⁶ mee te delen, geldig is of moet worden geconcludeerd dat de GGB een OCAD-gegevensbank is die toegankelijk is voor andere diensten. Het ontwerp zal daarom worden beoordeeld op basis van de ene of de andere hypothese.

II.5. Bewaartermijn van de verwerkte gegevens

112. Krachtens artikel 5.1.e) van de AVG, 28, 5° en 77 van de WVG mogen persoonsgegevens niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren, dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor ze worden verwerkt.

113. De maximale bewaartermijn voor gegevens is 60 jaar «*na de laatste verwerking*» (art. 7 van het wetsontwerp)¹⁴⁷.

¹⁴³ Natuurlijk is het identificeren van een gegevensbeheerder voor een gegevensbank op zichzelf geen slechte praktijk.

¹⁴⁴ Zonder afbreuk te doen aan de kritiek die supra is geuit bij de analyse van de doeleinden.

¹⁴⁵ Bedoeld in art. 31 ev. van het wetsontwerp (zie hierover *infra*)

¹⁴⁶ Heeft OCAD bijvoorbeeld het recht om gegevens verkregen van Consulaire Zaken door te geven aan buitenlandse diensten die niet de tegenhanger zijn van Consulaire Zaken ?

¹⁴⁷ De archiveringsperiode wordt echter verkort voor entiteiten die een vooronderzoek ondergaan (zie hierboven) en het is de bedoeling dat de archivering na 15 jaar plaatsvindt voor minderjarigen.

114. Deze termijn wordt verklaard door de praktijk van archivering (in handen van de verwerkingsverantwoordelijke en niet door verzending naar het Algemeen Rijksarchief) die krachtens dezelfde bepaling uiterlijk plaatsvindt 30 jaar «*na de laatste verwerking*».
115. Ten eerste is de Autoriteit van mening dat het criterium «*laatste verwerking*» ertoe zou kunnen leiden dat dit een onbeperkte opslag van de betrokken persoonsgegevens rechtvaardigt. De Autoriteit beveelt daarom aan om een objectief criterium te overwegen, zoals de meest recent onderzoeksverplichting met betrekking tot de betrokken entiteit.
116. Ten tweede is de Autoriteit van mening dat, aangezien de gegevens ten minste gedeeltelijk worden bewaard door elk van de diensten in de strafrechtelijke en veiligheidsketen, de noodzaak en evenredigheid van afzonderlijke archivering op GGB-niveau moet worden aangetoond. In ieder geval is de Autoriteit van mening dat moet worden bepaald dat deze gearchiveerde gegevens niet langer mogen worden meegedeeld aan andere diensten dan leden van de strafrechtelijke en veiligheidsketen (voor zover artikel 7, §2, 2° dit niet volledig lijkt uit te sluiten).
117. De Autoriteit merkt ook op dat de archiveringsperiode als maximum is vastgesteld. De mogelijkheid van vroegtijdige verwijdering moet daarom worden onderworpen aan voorwaarden (zoals het geval is voor archivering)¹⁴⁸.
118. Gezien het belang van de gevolgen die verbonden zijn aan de verwerking van deze gegevens (en in het bijzonder voor kwetsbare personen die hun recht om in beroep te gaan alleen ten koste van zeer aanzienlijke moeilijkheden kunnen uitoefenen), is de Autoriteit van mening dat de omstandigheden van de opslag in de GGB of in de archieven van de GGB regelmatig moeten worden gecontroleerd¹⁴⁹. De Autoriteit beveelt een jaarlijkse audit en archivering aan na 5 jaar van onsuccesvolle verificaties (of bij afwezigheid van een regelmatige verificatie tijdens de laatste 5 jaar), op voorwaarde dat de noodzaak van een ander tijdschema wordt aangetoond. Aan de andere kant kunnen meer gespreide verificaties acceptabel zijn voor wissing.

**Om deze redenen,
is de Autoriteit de volgende mening toegedaan:**

¹⁴⁸ Namelijk, als de persoonsgegevens niet langer rechtstreeks verband houden met een van de doeleinden die worden genoemd in artikel 5, lid 2

¹⁴⁹ Het ontwerp voorziet nu in 5 jaar (en 3 jaar voor minderjarigen).

- het lot van de 47 partnerdiensten met toegang tot de GGB moet worden verduidelijkt (punt 11) ;
- de delegaties in artikelen 6, 9, 33 en 40 van het wetsontwerp moeten beperkt blijven tot de wijze van uitvoering van de essentiële elementen die in het wetsontwerp moeten worden opgenomen (punt 21);
- de in artikel 8 aan de Koning verleende machtiging moet worden geschrapt en er moet worden bepaald dat «*elke verwerking van de gegevens in de gemeenschappelijke gegevensbank, met inbegrip van de registratie ervan, wordt onderworpen aan logging*» (punt 22) ;
- « het "extraheren" van lijsten (bedoeld in art. 26, §1) door diensten met een leesrecht moet in een logbestand worden opgenomen (punt 23) ;
- de organieke normen van de diensten met schrijfrecht moeten bepalen dat het verzamelen van gegevens en die waarschijnlijk in de GGB zullen worden geregistreerd, in een logbestand moeten worden opgenomen (punt 24) ;
- periodieke controle van logbestanden moet worden voorzien in het ontwerp en in de organieke normen van de partnerdiensten voor "lokale" verwerking (punt 25) ;
- strategische, tactische en operationele vereisten moeten van elkaar worden onderscheiden en nauwkeurig worden beschreven in de wet of een uitvoeringsbesluit (punt 30) ;
- de doeleinden die verband houden met het creëren van een gegevensbank moeten worden onderscheiden van de doeleinden van de verschillende verwerkingen die door elk van de diensten met betrekking tot deze gegevens worden uitgevoerd (punt 31) ;
- het commentaar op art. 6 moet voor elk van de diensten met een schrijfrecht aantonen dat het doel van elke verdere verwerking van deze gegevens verenigbaar is met het doel waarvoor ze zijn verzameld (punt 32) ;
- artikel 6 en het bijbehorende commentaar (evenals, indien van toepassing, de organieke normen van partnerdiensten) moeten worden aangepast vanuit het oogpunt van het doel van de verwerking en de noodzakelijke en evenredige aard ervan (punten 35 en 36) ;
- de doeleinden van toegang door partnerdiensten moeten worden bepaald voor elke gegevenscategorie (punt 37) ;
- de vaststelling van grenzen of vermelding in de toelichting van de omstandigheden waarin de verwerking van het doel zou afwijken, is wenselijk (punt 39);
- Artikel 9 van het ontwerp moet bepalen dat de koppeling van de GGB met authentieke bronnen in geen geval mag toelaten dat overheden die geen legale toegang hebben tot deze bronnen, toegang krijgen tot de gegevens in deze authentieke bronnen (punt 40) ;
- artikel 31 van het wetsvoorstel moet worden geherformuleerd om het in overeenstemming te brengen met zijn commentaar (punt 44);

- de doeleinden waarvoor gegevens worden meegedeeld aan diensten die worden uitgenodigd om deel te nemen aan een LTF, moeten worden gespecificeerd (punt 46) ;
- er moet worden nagegaan of de LTF's overlegplatforms zijn die georganiseerd zijn overeenkomstig artikel 458ter van het Strafwetboek, in welk geval de Autoriteit wenst dat het aangepaste ontwerp opnieuw aan haar wordt voorgelegd voor advies alvorens het wordt goedgekeurd (punt 47) ;
- als de aanvrager een nieuwe wettelijke uitzondering op het beroepsgeheim wil creëren, moet het commentaar bij artikel 19 opnieuw worden geformuleerd en moet het Strafwetboek worden gewijzigd om dit nieuwe type uitzondering in te voeren (punt 49) ;
- in voorkomend geval moet worden vastgesteld wat de bestemming van de onder het beroepsgeheim vallende informatie met de meegedeelde gegevens kan en/of moet doen (punt 50) ;
- indien de aanvrager voornemens is deze bepaling op andere partijen en/of overheden toe te passen, moet in het commentaar bij artikel 19 worden gespecificeerd welke partijen en op welke wijze;
- in voorkomend geval moet worden gespecificeerd welke gegevens van deelnemers aan een LIVC-overleg waarschijnlijk zullen worden verwerkt voor handavingsdoeleinden (punt 53) ;
- er moet een verwijzing naar de voorbereidende werkzaamheden van de wet van 2014 worden opgenomen in het commentaar bij artikel 7 en wat betreft het doel van de verwerking van gearchiveerde gegevens, moet het legitieme karakter ervan worden aangetoond (punt 57) ;
- aan de hand van de formulering van het doel van de verdere verwerking als bedoeld in de artikelen 4, 24, 28 en 46 moet kunnen worden vastgesteld of deze verenigbaar is met het doel waarvoor de gegevens oorspronkelijk zijn verzameld (punt 58) ;
- er moet worden vermeld (in art. 4 van het ontwerp) dat statistieken zullen worden opgesteld met het oog op de publicatie van een evaluatieverslag over de doeltreffendheid van de verwerkingsmiddelen die zijn geïmplementeerd en de autoriteiten die betrokken zijn bij het wetsontwerp en het uitvoeringsbesluit ten overstaan van de doeleinden waarvoor de gegevens zijn geregistreerd in de GGB (punten 59, 78, 81 en 97) ;
- de impact van het ontwerp op de werking van LIVC-R moet worden verduidelijkt (punten 61-63) ;
- de mogelijkheid om een informatiekaart aan een derde overheid of instelling door te geven, moet anders worden geformuleerd (punten 65 en 66) ;
- de rechtsgrondslag en de grenzen van de delegatie aan de Koning van de precisering van de mededelingsdoeleinden aan de burgemeesters, moeten worden vermeld (punt 67) ;
- art. 12 van het ontwerp KB moet worden afgestemd op het verslag aan de Koning (punt 69) ;

- de hoedanigheid op grond waarvan een burgemeester een bestemming van persoonsgegevens kan zijn, moet worden vastgesteld (punten 70 en 71) ;
- met betrekking tot de bevoegdheid van de burgemeester zoals omschreven in de nieuwe gemeentewet, moet worden verwezen naar "*bestuurlijke politiemaatregelen*" (punt 72) ;
- in voorkomend geval moet het ontwerp worden aangepast om de doeleinden van de verwerking te specificeren met betrekking tot de wettelijke bevoegdheden van de burgemeester om overleg te plegen over zaken in de zin van artikel 458 van het Strafwetboek (punt 73) ;
- de memorie van toelichting bij het ontwerp moet een rechtvaardiging bevatten van het noodzakelijke en evenredige karakter van de deelname van elk van de nieuwe partners, evenals van de voortzetting van elk van de diensten die momenteel deelnemen, met betrekking tot de mogelijkheid om het beoogde doel te bereiken door de mededeling van bepaalde gegevens door één van de basisdiensten alleen (punten 79 en 80) ;
- het aantonen van de noodzakelijke en evenredige aard van de mededeling zal ook betrekking moeten hebben op de modaliteiten van die mededeling (punt 82) ;
- de noodzaak om gegevens te communiceren met andere partners dan VSSE, OCAD en de federale politie wordt niet uitgedrukt of aangetoond (punt 87) ;
- de noodzakelijke en evenredige aard van de deelname van VZ aan de LTF's wordt niet aangetoond in de huidige staat van het ontwerp en lijkt niet aantoonbaar aan de hand van het geval dat in de toelichting wordt aangehaald (paragraaf 89) ;
- het verplicht voorafgaand overleg moet worden onderscheiden van het in real time of a posteriori verstrekken van informatie over het nemen van een maatregel, aan de diensten die over de gegevens van de betrokkene beschikken (punt 90) ;
- de diensten die kunnen worden uitgenodigd moeten op zijn minst vastgesteld kunnen worden (punt 91) ;
- Het begrip "*uitwisseling*" van gegevens moet worden verduidelikt (punt 92);
- Artikel 6 van het wetsontwerp moet worden geherformuleerd om - voor elk van de partnerdiensten - een onderscheid te maken tussen de categorieën gegevens waarover deze diensten beschikken en die zij op grond van dit ontwerp mogen meedelen "*met inachtneming van behoefte om te kennen*" van de andere diensten, en de gegevens die door andere deelnemers aan overlegvergaderingen worden meegedeeld en waarvan de andere deelnemende diensten kennis kunnen nemen (punt 95) ;
- wanneer het doel kan worden bereikt door gegevens van één dienst door te geven (bv. een uittreksel uit de dreigingsanalyse van OCAD of een verslag van de lokale politie), moet dit op die manier worden gedaan (punt 96) ;
- Er moet worden bepaald dat gegevens in politiegegevensbanken alleen door partnerdiensten mogen worden verwerkt als de juistheid ervan is vastgesteld door middel van een "*justitiële retourstroom*" (punt 98) ;

- Er moet worden bepaald dat minder ernstige veroordelingen die geen verband houden met de strafbare feiten van terroristische aard als bedoeld in titel I ter van boek II van het Strafwetboek, of zelfs zeer oude veroordelingen, niet door de partnerdiensten worden verwerkt (punt 99) ;
- art. 44/1, §3, 2° WPA moet worden opgenomen in het ontwerp (punt 100) ;
- het noodzakelijke en evenredige karakter van de verwerking van gegevens met betrekking tot politieke opvattingen en godsdienstige of levensbeschouwelijke overtuiging door elk van de diensten die er kennis van kunnen nemen, zal ook moeten worden aangetoond in het commentaar bij artikel 6 (punt 101) ;
- een beschrijving van de technische en organisatorische maatregelen die ervoor moeten zorgen dat gegevens die door de bevoegde dienst worden doorgegeven voor een doel dat verband houdt met het voorkomen van terrorisme, niet voor andere doeleinden door andere autoriteiten kunnen worden verwerkt, moet in het ontwerp worden opgenomen (punt 102) ;
- in de toelichting bij artikel 24 moet duidelijk worden gemaakt dat het er niet om gaat de "andere bestemmingen" van de informatiekaart toe te staan van deze bepaling gebruik te maken om "onderzoek" te doen, of om de gegevens die zij over de "entiteiten" hebben, te consolideren met informatie die voor hun eigen doeleinden irrelevant zou zijn (punt 103) ;
- de noodzakelijkheid en evenredigheid van de verwerking van persoonsgegevens van entiteiten moet per dienst worden aangetoond (punt 104) ;
- de verwerking van persoonsgegevens van minderjarige kinderen van bepaalde entiteiten overstijgt de doeleinden van registratie in een gegevensbank die toegankelijk is voor diensten die andere taken hebben dan die van de inlichtingendiensten (punt 105) ;
- het moet in het wetsontwerp heel duidelijk worden gemaakt aan welke autoriteit of autoriteiten de GGB rapporteert (of bij welke autoriteiten de GGB is opgericht) en waarom (punt 108) ;
- het is noodzakelijk om in het ontwerp te bepalen wie de verantwoordelijken voor de verwerking zijn, op basis van de verschillende verwerkingen die waarschijnlijk zullen worden uitgevoerd en niet op basis van de gegevensbank (punt 109) ;
- de redenen voor het gebrek aan afstemming tussen de basisdiensten/GGB-partners en de ambtshalve of uitgenodigde deelnemers aan de coördinatie van LTF moeten in detail worden uiteengezet in de memorie van toelichting (punt 110) ;
- in het commentaar bij artikel 28 moet worden gespecificeerd welke autoriteit onder de wettelijke verplichtingen (of de Verdragen) valt voor de mededeling van de gegevens uit de GGB (punt 111) ;
- het criterium "na de laatste verwerking" voor het bepalen van de maximale archiveringsperiode moet worden losgelaten (punt 115) ;

- de noodzaak en evenredigheid van gescheiden archivering op GGB-niveau moet worden aangetoond (punt 116) ;
- gearhiveerde gegevens mogen niet langer kunnen worden meegedeeld aan andere diensten dan de leden van de strafrechtelijke en veiligheidsketen (punt 116) ;
- er moeten voorwaarden worden verbonden aan de mogelijkheid van vroegtijdige wissing (punt 117) ;
- de bewaaromstandigheden in de GGB of in de archieven van de GGB moeten regelmatig worden geverifieerd (punt 118).



Voor het Kenniscentrum,
Cédrine Morlière, Directeur



ANNEX

Belangrijkste afkortingen:

GGB	Gemeenschappelijke gegevensbank
BELPIU	Passagiersinformatie-eenheid
C.O.C.	Controleorgaan op de politionele informatie
VCLP	Vaste Commissie van de Lokale Politie
Comité I	Vast Comité van toezicht op de inlichtingendiensten
LIVC-R	Lokale integrale veiligheidszellen inzake radicalisme, extremisme en terrorisme
PGE	Potentieel geweldadige extremisten
ETIAS	European Travel Information and Authorisation System
FTF	Foreign terrorist fighters
GPI	Geïntegreerde politie
HTF	Homegrown terrorist fighters
WPA	Wet op het politieambt
OCAD	Coördinatieorgaan voor de dreigingsanalyse.
VZ	Dienst Vreemdelingenzaken
HP	Haatpropagandisten
ADIV	Algemene Dienst Inlichting en Veiligheid.
T.E.R.	Terrorisme, extremisme en radicalisme
LTF	Local Task Force
VSSE	Veiligheid van de staat



ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
	DA230014		20.06.2023

Objet : Avis relatif 1) à l'avant-projet de loi portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. ») et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police et 2) au projet d'arrêté royal relatif à la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. »)

L'Organe de contrôle de l'information policière (ci-après le 'COC' ou 'l'Organe de contrôle').

Vu la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (M.B. du 5 septembre 2018, ci-après 'la LPD'), en particulier l'article 59 §1^{er}, 2^e alinéa, l'article 71 et le Titre VII, en particulier l'article 236.

Vu la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après 'la LAPD').

Vu la loi du 5 août 1992 sur la fonction de police (ci-après 'la LFP').

Vu la *Law Enforcement Directive* 2016/680 du 27 avril 2016 (ci-après 'la LED').

Vu la demande du ministre de la Justice du 14 avril 2023 en vue d'émettre un avis concernant 1) l'avant-projet de loi portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. ») et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police et 2) le projet d'arrêté royal relatif à la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. »).

Vu le rapport de Monsieur Koen Gorissen, membre-conseiller de l'Organe de contrôle.

Émet, le 20 juin 2023, l'avis suivant.

I. Remarque préalable concernant la compétence de l'Organe de contrôle

1. À la lumière respectivement de l'application et de la transposition du Règlement 2016/679¹ et de la Directive 2016/680², le législateur a remanié en profondeur les tâches et missions de l'Organe de contrôle. L'article 4 §2, quatrième alinéa de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après 'la LAPD') dispose qu'à l'égard des services de police au sens de l'article 2, 2^o, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle. Cela signifie notamment que l'Organe de contrôle est compétent également lorsque des services de police traitent des données à caractère personnel qui ne relèvent pas des missions de police administrative et judiciaire, par exemple dans le cadre de finalités socioéconomiques ou de traitements relevant de la gestion des ressources humaines. L'Organe de contrôle doit être consulté lors de la préparation de la législation ou d'une mesure réglementaire ayant trait au traitement de données à caractère personnel par les services de police de la police intégrée (voir les articles 59 §1^{er}, 2^e alinéa et 236 §2 de la LPD, l'article 36.4 du RGPD et l'article 28.2 de la directive Police-Justice ou *LED*). L'Organe de contrôle a dans ce contexte pour mission d'examiner si l'activité de traitement projetée par les services de police est conforme aux dispositions du Titre 1^{er} (pour les traitements non opérationnels)³ et du Titre 2 (pour les traitements opérationnels) de la LPD⁴. De plus, le COC est aussi chargé d'émettre des avis d'initiative, comme prévu à l'article 236 §2 de la LPD, et est investi conformément à l'article 240 de la LPD d'une mission générale d'information à l'égard du grand public, des personnes concernées, des responsables du traitement et des sous-traitants dans le domaine du droit à la protection des données et à la protection de la vie privée.

2. En ce qui concerne en particulier les activités de traitement dans le cadre des missions de police administrative et/ou judiciaire, l'Organe de contrôle émet dès lors des avis soit d'initiative, soit à la demande du Gouvernement ou de la Chambre des Représentants, d'une autorité administrative ou judiciaire ou d'un service de police, concernant toute matière ayant trait à la gestion de l'information policière telle que régie par la Section 12 du Chapitre 4 de la loi sur la fonction de police⁵.

¹ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE » (règlement général sur la protection des données ou « RGPD »).

² Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil » (ci-après dénommée « directive Police-Justice » ou *Law Enforcement Directive (LED)*).

³ Article 4 §2, 4^e alinéa de la LPD.

⁴ Article 71 §1^{er}, 3^e alinéa de la LPD.

⁵ Articles 59 §1^{er}, 2^e alinéa et 236 §2 de la LPD.

3. Par ailleurs, l'Organe de contrôle est également chargé, à l'égard des services de police, de l'inspection générale de la police fédérale et de la police locale (en abrégé 'AIG') visée dans la loi du 15 mai 2007 sur l'Inspection générale et de l'Unité d'information des passagers (ci-après dénommée en abrégé 'BELPIU') visée au Chapitre 7 de la loi du 25 décembre 2016, de la surveillance de l'application du Titre 2 de la LPD et/ou du traitement de données à caractère personnel tel que visé aux articles 44/1 à 44/11/13 de la loi sur la fonction de police, et/ou de toute autre mission qui lui est confiée en vertu ou par d'autres lois⁶.

4. L'Organe de contrôle est compétent à l'égard du Service Contentieux de l'Administration générale des Douanes et Accises en ce qui concerne les réquisitions adressées par ce service à la BELPIU dans des matières fiscales, et ce en vertu de l'article 281 §4 de la loi générale « *sur les douanes et accises* » du 18 juillet 1977, telle que modifiée par la loi du 2 mai 2019 « *modifiant diverses dispositions relatives au traitement des données des passagers* ».

5. Enfin, l'Organe de contrôle est également chargé, dans le cadre de la législation sur la rétention des données et en vertu de l'article 126/3 §1^{er}, 8^e alinéa de la loi du 13 juin 2005 relative aux communications électroniques (ci-après 'la LCE'), telle que modifiée par la loi du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités (M.B. du 8 août 2022), de la validation des statistiques relatives au nombre de faits punissables et au délai de conservation pour chaque arrondissement judiciaire et chaque zone de police, une matière dans le cadre de laquelle il exerce toutes les compétences qui lui ont été attribuées par le Titre 7 de la loi du 30 juillet 2018. Il est par ailleurs également chargé, en application de l'article 42 §3, 2^e et 3^e alinéas de la LFP, du contrôle des requêtes de la Cellule Personnes disparues de la police fédérale en vue de la consultation des données relatives aux communications électroniques impliquant la personne disparue.

6. L'Organe de contrôle est compétent pour rendre des avis sur les aspects ayant trait au traitement des informations et des données à caractère personnel et à la protection de la vie privée par le traitement de données à caractère personnel pour autant qu'il existe un rapport avec le fonctionnement opérationnel et non opérationnel des services de police et/ou avec le personnel de la police intégrée (ci-après 'la GPI⁷') et/ou pour autant que le projet de texte soumis pour avis ait un impact sur la gestion de l'information policière en général.

7. Par ailleurs, l'Organe de contrôle n'est pas seulement une autorité de protection des données, mais est aussi une autorité de contrôle qui est légalement chargée de contrôler la légalité, l'efficacité, l'efficience et l'économie de la gestion de l'information policière⁸.

⁶ Article 71 §1^{er}, troisième alinéa *juncto* article 236 §3 de la LPD.

⁷ Geïntegreerde politie – Police Intégrée.

⁸ Rapport d'activité 2021, www.organedecontrole.be, voir les points 3 et 52 et plus spécifiquement le point 71 : « *Il serait cependant faux de s'imaginer que le COC se préoccupe seulement de la protection des données ; il porte aussi énormément*

II. Objet de la demande

8. La demande d'avis a trait 1) à l'avant-projet de loi portant création de la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. ») et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police (ci-après 'le projet de loi T.E.R.') et 2) au projet d'arrêté royal relatif à la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » (« T.E.R. ») (ci-après 'le projet d'arrêté royal T.E.R.'). Les deux textes étant étroitement liés, ils sont traités ensemble dans le présent avis.

9. Conformément à l'exposé des motifs, le projet de loi T.E.R. vise à transposer dans une loi autonome les dispositions de la loi du 5 août 1992 sur la fonction de police relatives aux banques de données communes 'Terrorist Fighters' et 'Propagandistes de haine', dont les modalités de traitement sont détaillées dans l'arrêté royal du 21 juillet 2016 « *relatif à la banque de données commune 'Terrorist Fighters'* » et dans l'arrêté royal du 23 avril 2018 « *relatif à la banque de données commune 'Propagandistes de haine' et portant exécution de certaines dispositions de la section 1^{re}bis « de la gestion des informations » du chapitre IV de la loi sur la fonction de police* ».

Selon l'exposé des motifs, ce projet de loi permet de rationaliser un certain nombre de règles en fusionnant dans un même instrument juridique les banques de données communes 'Terrorist Fighters' et 'Propagandistes de haine'. Un travail de réécriture a également été déployé pour clarifier les processus, des définitions ont été ajoutées ou réécrites, les finalités ont été ajustées et bon nombre de dispositions jugées essentielles des arrêtés royaux ont été ramenées au niveau de la loi. Le projet ajoute encore des dispositions en matière de protection des données à caractère personnel, met en place un mécanisme de concertation systématique au niveau du suivi des entités et entérine l'existence des Task Forces Locales (LTF) et détermine leurs missions.

10. L'exposé des motifs évoque les raisons suivantes pour motiver la création d'une loi autonome pour la banque de données commune « Terrorisme, Extrémisme, processus de Radicalisation » :

- répondre à une demande émanant tant de la Commission d'enquête parlementaire que de l'Autorité de protection des données (ci-après 'l'APD') visant à donner une base juridique *ad hoc* à cette banque de données, qui n'avait pas de raison spécifique d'être attachée à la LFP ;

d'attention à tous les autres aspects opérationnels de la gestion de l'information policière et des informations des autres services qu'il contrôle, s'agissant là de matières relevant également de sa compétence. » ; article 71 §1^{er} de la LPD.

- la nécessité, après l'affaire Conings, d'obliger la Task Force Locale à parcourir une liste de mesures qui peuvent être prises à l'égard d'une entité ;
- la nécessité, par suite du décès tragique d'un policier, de permettre aux services de base de communiquer certaines données de la banque de données T.E.R. aux professionnels des soins de santé.

La majorité des articles de la LFP ou des arrêtés royaux 'TF' et 'PH' existants et en vigueur a été transférée dans le projet de loi sans modification de fond. Seules les nouvelles dispositions sont développées et explicitées dans l'exposé des motifs. Pour le reste, il est renvoyé aux travaux parlementaires de la loi du 27 avril 2016 relative à des mesures complémentaires en matière de lutte contre le terrorisme et aux rapports au Roi des arrêtés royaux d'exécution précités.

Le projet d'arrêté royal, enfin, a conformément au rapport au Roi pour objectif de développer certains aspects de la banque de données commune T.E.R. créée par le projet de loi T.E.R.

Étant donné que les deux projets ont un impact sur la gestion de l'information par la GPI, l'Organe de contrôle se limitera dans le présent avis aux aspects du projet qui ont trait à cette matière. Pour le reste, l'Organe de contrôle renvoie à l'avis de l'APD ainsi qu'à ses avis et rapports antérieurs⁹ concernant les banques de données communes 'TF' et 'Propagandistes de haine'.

III. Analyse de la demande

A. Généralités

11. L'Organe de contrôle salue la transposition dans une loi autonome des dispositions de la LFP relatives aux banques de données communes 'Terrorist Fighters' et 'Propagandistes de haine'. Ce fondement juridique *ad hoc* est un choix logique pour de telles banques de données (communes) accessibles à plusieurs services, qui ne doivent pas nécessairement – et même de préférence pas – être reprises dans la LFP vu qu'il ne s'agit pas de banques de données purement policières (comme toutes les autres, notamment les banques de données de base, la BNG, les banques de données particulières et les banques de données techniques). De plus, la création de cette loi autonome et la reprise dans celle-ci des principaux éléments des arrêtés d'exécution permettent de mettre en place une base juridique plus solide.

12. L'Organe de contrôle constate également que l'auteur du projet a mis l'occasion à profit pour se pencher sur certains aspects de la réglementation existante et en évaluer la nécessité. Certains

⁹ Voir les rapports conjoints de l'Organe de contrôle de l'information policière et du Comité permanent R concernant la banque de données commune TF établis en 2017, 2018, 2019 et 2020, ainsi que les avis relatifs aux déclarations préalables de la banque de données commune TF (non publiés).

services partenaires, notamment, n'ont plus été repris dans la liste actuelle des services partenaires du projet de loi en raison de l'absence dans leur chef d'un 'besoin d'en connaître'. Dans leurs rapports conjoints de 2018 et 2019 concernant la banque de données commune 'TF' (BDC TF), le COC et le Comité permanent R évoquaient déjà la problématique de la révision de l'accès de certains anciens services partenaires en raison de l'absence dans leur chef d'un 'besoin d'en connaître', et ce notamment parce qu'il n'a pendant plusieurs années pas été désigné d'utilisateur pouvant accéder à la BDC TF.

13. Le type spécifique d'accès (droits de création, de lecture, d'écriture et d'interrogation¹⁰) des différents services partenaires n'est pas spécifié dans le projet de loi, mais est laissé à l'appréciation du Roi. **Cependant, il serait indiqué de prévoir dans le projet de loi lui-même le type spécifique d'accès à la banque de données commune ainsi que le cadre dans lequel le service partenaire concerné pourra exercer ces droits, s'agissant là d'un élément essentiel du traitement de données à caractère personnel¹¹.**

Étant donné que la majorité des articles de la LFP ou des arrêtés royaux TF a été transférée dans le projet de loi et/ou dans le projet d'arrêté royal sans modification de fond, l'Organe de contrôle analysera ci-après en particulier les nouveaux articles ou les articles ayant été modifiés en profondeur qui ont un impact notable sur la gestion de l'information par la GPI.

B. Commentaire des articles du projet de loi T.E.R.

14. L'article 6 §2, 2° du projet de loi dispose que les données à caractère personnel traitées dans la banque de données commune T.E.R. sont : « (...) *les données administratives, judiciaires, (...) de police judiciaire, de police administrative et les informations relatives aux entités enregistrées, traitées conformément à la loi par les services de base et les services partenaires qui disposent d'un droit de lecture et d'un droit d'écriture dans la banque de données commune T.E.R. et qui sont adéquates, pertinentes et non excessives au regard des missions visées à l'article 3 et des finalités visées à l'article 5, alinéa 2* ».

¹⁰ Voir l'article 2 du projet de loi, 11°-14°.

¹¹ Encore récemment, la Cour constitutionnelle s'est prononcée à ce sujet en ces termes dans son arrêt du 10 mars 2022 (Cour constitutionnelle, arrêt n° 33/2022 du 10 mars 2022, considérant B.13.1, www.const-court.be/fr/) : « L'article 22 de la Constitution réserve au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée. Il garantit ainsi à tout citoyen qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue.

...

Par conséquent, les éléments essentiels des traitements de données à caractère personnel doivent être fixés dans la loi elle-même¹². A cet égard, quelle que soit la matière concernée, constituent, en principe, des éléments essentiels, les éléments suivants : 1°) les catégories de données traitées ; 2°) les catégories de personnes concernées ; 3°) la finalité poursuivie par le traitement ; 4°) les catégories de personnes ayant accès aux données traitées et 5°) le délai maximal de conservation des données (avis de l'assemblée générale de la section de législation du Conseil d'État n° 68.936/AG du 7 avril 2021 sur un avant-projet de loi « relative aux mesures de police administrative lors d'une situation d'urgence épidémique », Doc. parl., Chambre, 2020-2021, DOC 55-1951/001, p. 119) » (considérant B.13.1).

Pour la GPI, il s'agit donc de données de police judiciaire et administrative, mais uniquement après qu'il a été évalué si elles sont adéquates, pertinentes et non excessives au regard des missions et des finalités du projet de loi, comme le souligne aussi l'exposé des motifs. En sa qualité de service de base, la GPI dispose d'un droit de création d'une entité dans la BDC T.E.R., de sorte qu'elle devra lors de la création tenir compte de ces éléments. Conformément à l'article 18 du projet de loi, les modalités d'exercice du droit de création sont déterminées par le Roi (en particulier à l'article 14 du projet d'arrêté royal relatif à la validation interne). Une telle évaluation au regard des missions et des finalités du projet de loi devra donc être incluse dans la validation interne, d'autant plus que la nature des informations policières pouvant être transmises à la BDC T.E.R. n'est pas limitée.

Les *données de police administrative et judiciaire* constituent en effet une catégorie très vaste et très diverse de données (à caractère personnel). Cela signifie *de facto* que pour ainsi dire l'ensemble de la BNG Administratif et de la BNG Judiciaire peut faire l'objet d'un enregistrement dans la BDC, de même que toutes les informations et données à caractère personnel des banques de données de base, des banques de données particulières et des banques de données techniques. Le projet de loi ne tient aucunement compte du statut de validation des données à caractère personnel et informations policières. Les informations brutes – qui n'ont pas fait l'objet d'un processus de validation –, comme celles qui figurent dans les banques de données de base, font également ou peuvent également faire l'objet d'un enregistrement dans la BDC T.E.R. Tant les « informations dures » (procès-verbaux) que les « informations douces » (contenues dans les rapports d'information, autrement dit des faits non concrets) peuvent également en faire l'objet. Si telle n'était pas l'intention, il revient à l'auteur du projet de le préciser dans le projet de loi.

15. Dans l'intérêt de la personne concernée et du prestataire de soins, le service de base (dont la GPI) qui est en contact avec celui-ci lui communique conformément à l'article 6 §2, 3°, 2^e alinéa du projet de loi les données médicales nécessaires enregistrées dans la BDC T.E.R. et les données issues de l'évaluation de la menace relative à la dangerosité de la personne concernée. **Il est recommandé de prévoir que cette communication émanant de la GPI revête une forme écrite, de manière à éviter toute discussion par la suite. Voir aussi plus loin le point 24.**

16. L'article 7 dispose qu'après le dernier traitement, le responsable opérationnel examine tous les cinq ans (tous les trois ans lorsque les données à caractère personnel sont relatives à des mineurs) si les données à caractère personnel présentent toujours un lien direct avec l'une des finalités de l'article 5 du projet de loi. Si tel n'est pas le cas, les données sont archivées. Le projet de loi prévoit une durée d'archivage de maximum 30 ans, par analogie avec ce que prévoit la LFP¹². Un tel délai de conservation

¹² Voir par exemple l'article 44/10 de la loi sur la fonction de police en ce qui concerne l'archivage des données à caractère personnel et informations dans la BNG.

supplémentaire sous la forme d'un archivage de maximum 30 ans semble difficilement tenable vu la jurisprudence récente¹³ de la Cour de Justice de l'Union européenne et les principes du droit à la protection des données (données 'adéquates, pertinentes et non excessives', comme le précise d'ailleurs le projet de loi). Il semble donc contradictoire de vouloir archiver les données si elles ne présentent plus de lien avec l'une des finalités de l'article 5 du projet de loi, au lieu de les effacer parce qu'elles ne sont plus adéquates, pertinentes et non excessives. **L'auteur du projet doit par conséquent y réfléchir et au moins procéder à une évaluation critique du système d'archivage projeté, qui constitue une copie de ce qui est prévu dans la LFP.**

Dans leurs rapports du contrôle conjoint de la BDC TF, l'Organe de contrôle et le Comité permanent R ont insisté à plusieurs reprises sur la nécessité de respecter rigoureusement ces délais, et ce en développant à cette fin un outil informatique. Les autorités de contrôle (le COC et le Comité permanent R) doivent en effet pouvoir vérifier le respect de ces délais. **Il est par conséquent recommandé de prévoir dans le projet de loi que le responsable opérationnel reprenne cette évaluation dans le dossier de l'entité concernée, de manière à ce qu'il soit possible pour les autorités de contrôle de vérifier l'évaluation et le délai, et de suivre rigoureusement ces délais dans une application informatique.**

17. L'article 9 du projet de loi prévoit la possibilité d'établir une interconnexion entre la BDC T.E.R. et d'autres banques de données gérées par les services de base ou les services partenaires. Conformément à la définition énoncée à l'article 2, 16° du projet de loi, une telle interconnexion implique notamment que les données à caractère personnel et les informations pertinentes des banques de données, sources authentiques peuvent être transférées vers la BDC T.E.R.

Pour la GPI, cela signifie par exemple une interconnexion avec la BNG et toutes les autres banques de données policières. On peut toutefois s'interroger sur le rapport entre cet article du projet de loi et les dispositions des articles 44/11/4 et suivants de la LFP. **Il appartient à l'auteur du projet de faire la clarté sur ce point.**

L'article 9 dispose par ailleurs que le Roi détermine dans les cas susmentionnés les finalités de l'interconnexion, les catégories de données à caractère personnel interconnectées et les modalités d'interconnexion, lesquelles doivent respecter l'intégrité des données et des réseaux. **Il convient de solliciter en la matière l'avis préalable des autorités de contrôle au sujet de l'arrêté royal susmentionné, et notamment de l'Organe de contrôle en sa qualité d'autorité de contrôle compétente pour les services de police, conformément à l'article 26, 7°, a) de la LPD.**

¹³ Cour de Justice de l'Union européenne, 21 juin 2022, dossier C-817/19.

18. L'article 17 régit les droits d'accès possibles (droit de lecture, droit d'écriture ou droit d'interrogation) pour les services partenaires, mais laisse au Roi le soin d'en déterminer les modalités. L'exposé des motifs indique qu'il a été opté pour un arrêté royal afin de conserver une certaine flexibilité dans l'octroi, le retrait ou la modification de l'accès en fonction de l'évolution des compétences, des missions et des besoins des différents services partenaires. **Toutefois, comme le COC l'a déjà fait remarquer au point 13, il est indiqué de prévoir dans le projet de loi lui-même le type spécifique d'accès à la banque de données commune ainsi que le cadre dans lequel le service partenaire concerné pourra exercer ces droits. Les BDC TF et PH sont dans l'intervalle opérationnelles depuis plusieurs années, de sorte que l'on devrait en tout cas connaître les besoins des missions et nécessités respectives des différents services partenaires.**

19. Conformément à l'article 19 du projet de loi, les services de base – dont la GPI – sont tenus respectivement de consulter la banque de données commune T.E.R. et d'y introduire d'office leurs propres données à caractère personnel et les informations pertinentes. Ces données sont enregistrées dans la BDC sous leur responsabilité et suivant leurs procédures internes de validation. Ces données à caractère personnel et informations proviennent des données à caractère personnel et informations qui sont à disposition des services de base et des services partenaires dans le cadre de leurs missions respectives et des finalités qui y sont liées. **Il peut à ce sujet être fait référence aux remarques formulées au point 14.**

Le 4^e alinéa de l'article 19 prévoit en outre que la GPI saisit les données à caractère personnel et les informations conformément aux spécifications supplémentaires énoncées dans une directive du Collège des procureurs généraux. Par ailleurs, l'article 20 dispose que le droit de création et le droit d'écriture dans la BDC T.E.R. sont différés lorsque et aussi longtemps que le magistrat compétent estime que cette création et cette alimentation peuvent compromettre l'exercice de l'action publique, la sécurité d'une personne ou la relation avec un service répressif d'un État étranger. Dans leurs rapports antérieurs au sujet de la BDC TF, le COC et le Comité permanent R ont épinglé le fait que les informations policières provenant de « RIR, codes 01 ou 00 » ne sont pas enregistrées dans la BDC. Un « RIR 01 » a trait à des informations policières qui ne peuvent être utilisées qu'avec l'accord du verbalisateur, tandis qu'un « RIR 00 » a trait à des informations policières qui ne peuvent en aucun cas être utilisées. Il s'agit d'informations sensibles (mais n'ayant pas été classifiées) qui peuvent par exemple conduire à l'identification d'une source. Ces codes sont le résultat d'une directive ministérielle qui n'a été publiée qu'en partie et dans une mesure très restreinte, à savoir la directive MFO-3, qui a trait notamment à la saisie de données dans la Banque de données nationale générale (BNG) de la police intégrée.

La réglementation ne prévoit pas d'exceptions en ce qui concerne la transmission de ce type d'informations policières à la BDC, de sorte que ces informations devraient obligatoirement être

enregistrées dans la BDC. En effet, sur le plan juridique, la LFP (dans le passé) et (à l'avenir) le projet de loi T.E.R. et ses arrêtés d'exécution ont priorité sur la directive MFO-3 en vertu du principe de la hiérarchie des normes (la MFO-3 se base en effet sur les dispositions en matière de gestion de l'information de la LFP). Ces dernières années, le COC et le Comité permanent R ont donc recommandé d'évaluer cette problématique et de remédier à cette situation. **Il appartient dès lors à l'auteur du projet de régler cet aspect dans le présent projet de loi, ou du moins de faire la clarté sur ce point par exemple dans l'exposé des motifs.**

20. L'article 22 du projet de loi prévoit que les autorités administratives compétentes sont informées par le chef de corps de chaque zone de police concernée en cas de création d'une nouvelle entité dans la BDC T.E.R. Peut-il s'agir aussi d'une nouvelle entité à propos de laquelle il existe conformément à l'article 2, 6° du projet d'arrêté royal de sérieux indices qu'elle puisse remplir les critères visés à l'article 1^{er}, 4°, 5°, 6° ou 8° du projet d'arrêté royal T.E.R. ? Dans le cas contraire, ces entités doivent en effet être archivées au bout de six mois conformément à l'article 13 du projet d'arrêté royal T.E.R. En d'autres termes, cela inclut-il également les 'entités test ou potentielles' ? Il se pourrait en effet qu'il apparaisse au bout de quelques mois qu'une telle 'entité test ou potentielle' ne peut pas être enregistrée dans la BDC T.E.R. **Il est indiqué de faire la clarté sur ce point. Pour autant que la disposition inclue également la catégorie susmentionnée d'entités qui s'avèrent au bout de six mois ne pas être validées, cette information de non-confirmation doit également être notifiée aux autorités administratives compétentes susmentionnées et il convient de veiller à ce que ces informations soient effacées auprès de cette entité administrative.**

21. Conformément à l'article 24 du projet de loi, une carte d'information peut être communiquée à une autorité tierce qui a le besoin d'en connaître, après évaluation par le gestionnaire, le responsable opérationnel et les services de base. Cette évaluation porte au minimum sur 4 éléments, à savoir 1) la contribution de l'autorité tierce à la prévention ou à la lutte contre le terrorisme et l'extrémisme pouvant mener au terrorisme, 2) le traitement ultérieur qui sera réalisé par l'autorité tierce eu égard à l'exercice de ses compétences et les risques éventuels pour les libertés et droits fondamentaux de la personne concernée, 3) la situation de vulnérabilité de la personne concernée, en ce compris la minorité de la personne, et 4) le caractère adéquat, pertinent et non excessif des catégories de données communiquées tenant compte du traitement ultérieur. Le COC et le Comité permanent R ont également formulé dans le passé des remarques quant à la licéité de cette transmission de listes. Le COC salue donc les dispositions prévues dans le projet de loi, et en particulier les critères minimaux pour l'évaluation d'une telle transmission. **Afin de permettre un contrôle efficace de cet aspect, l'auteur du projet est prié de prévoir explicitement que le responsable opérationnel tienne à jour pour les autorités de contrôle une liste de ces communications permettant de retrouver pour chaque transmission l'évaluation réalisée.**

22. Selon l'article 28 §2 du projet de loi, les données à caractère personnel et les informations de la BDC T.E.R. peuvent être communiquées conformément à l'article 44/11/13 de la LFP aux services de police étrangers et autorités judiciaires étrangères et aux organisations internationales de coopération judiciaire et policière. Le §4 dispose par ailleurs que le Roi peut déterminer les modalités de cette communication. **Ici aussi, il convient de solliciter en la matière l'avis préalable des autorités de contrôle au sujet de l'arrêté royal susmentionné, et notamment de l'Organe de contrôle en sa qualité d'autorité de contrôle compétente pour les services de police, conformément à l'article 26, 7°, a) de la LPD.**

23. L'article 30 prévoit que la responsabilité de la qualité des données à caractère personnel et des informations enregistrées dans la BDC T.E.R. incombe au responsable du traitement propre à chaque service qui alimente la BDC T.E.R. Pour la GPI et spécifiquement pour la BNG et les banques de données de base, cela signifie que les ministres de la Justice et de l'Intérieur sont les responsables du traitement. Or, ils sont également les responsables du traitement de la BDC T.E.R. elle-même en vertu de l'article 5 du projet de loi.

La notion de « responsable du traitement » est toutefois un concept fonctionnel visant à attribuer les responsabilités aux personnes qui exercent une influence de fait¹⁴. Concrètement, cela signifie que l'entité qui décide du 'quoi' et du 'comment' du traitement de données sera le responsable du traitement, indépendamment du statut ou de la position qui est attribué(e) à cette entité au sein de son organisation. La compétence de '*constater*' peut, il est vrai, être régie spécifiquement par la loi, mais ressort par ailleurs également des compétences qui sont attribuées à une certaine entité ou d'une analyse des faits et circonstances.

En ce sens, l'Organe de contrôle considère – et agit ainsi dans la pratique – les services de police, au niveau fédéral et local, comme étant le 'responsable opérationnel du traitement' car ils ont une influence factuelle déterminante sur le traitement (l'enregistrement) concret et effectif des données à caractère personnel et qu'ils en sont maîtres.

L'Organe de contrôle est demandeur¹⁵ de la traduction de cette réalité de terrain dans la loi sur la fonction de police. Un contrôle efficace par le COC et une législation correcte en matière de protection des données policières exigent, en termes de clarté juridique, que le responsable opérationnel du traitement soit en tant que tel défini par la loi.

¹⁴ Groupe de travail « Article 29 » sur la protection des données, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_fr.pdf, p. 12.

¹⁵ Voir aussi les avis rendus dans le cadre des dossiers DA220017 (SIS) et DA220030 (DPO), disponibles sur le site Internet de l'Organe de contrôle : <https://www.organedecontrôle.be/publications>.

Il est par conséquent indiqué de prévoir à l'article 30 du projet de loi, pour la GPI, des 'responsables du traitement opérationnels' qui assurent effectivement l'alimentation de la BDC T.E.R. et qui sont donc aussi les mieux placés pour répondre de la qualité des données à caractère personnel et des informations.

24. Enfin, l'article 53 du projet de loi prévoit l'insertion dans la LFP d'un article 44/11/9*bis* relatif à la communication, par la GPI, de données à caractère personnel et d'informations aux services de la santé, d'urgence et/ou de secours. **Comme nous le disions au point 15, il est indiqué de prévoir également que cette communication émanant de la GPI soit enregistrée, de manière à éviter toute discussion par la suite.**

25. Pour le reste, l'Organe de contrôle n'a pas d'autres remarques à formuler concernant le projet de loi T.E.R.

C. Commentaire des articles du projet d'arrêté royal T.E.R.

26. L'article 2, 6° du projet d'arrêté royal mentionne parmi les catégories d'entités traitées dans la BDC T.E.R. « *les entités à propos desquelles il existe de sérieux indices qu'elles puissent remplir les critères visés à l'article 1^{er}, 4°, 5°, 6° ou 8°* ». L'article 13 du projet d'arrêté royal prévoit que ces données sont conservées pour une durée de maximum six mois après leur enregistrement et sont archivées à l'issue de ce délai si elles ne répondent pas aux critères susmentionnés de l'article 1^{er}. **L'auteur du projet est par conséquent prié de mentionner ce délai également dans le projet de loi plutôt que dans le projet d'arrêté royal, dès lors qu'il s'agit d'un élément essentiel du traitement de données à caractère personnel.**

Dans leurs rapports du contrôle conjoint de la BDC TF, l'Organe de contrôle et le Comité permanent R ont insisté à plusieurs reprises sur la nécessité de respecter rigoureusement ces délais, et ce en développant à cette fin un outil informatique. Outre le responsable opérationnel, les autorités de contrôle (le COC et le Comité permanent R) doivent en effet pouvoir elles aussi vérifier le respect de ces délais. **L'auteur du projet est par conséquent prié de prévoir dans le projet d'arrêté royal que le responsable opérationnel reprenne cette évaluation dans le dossier de l'entité concernée, de manière à ce qu'il soit possible pour les autorités de contrôle de vérifier l'évaluation et le délai, et de suivre rigoureusement ces délais dans une application informatique.**

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

prie le demandeur de tenir compte des remarques susmentionnées.

Avis approuvé par l'Organe de contrôle de l'information policière le 20 juin 2023.

Pour l'Organe de contrôle,
Le Président a.i.,
Frank Schuermans (SIGNÉ)



CONTROLEORGaan OP DE POLITIE-INFORMATIE

Uw referentie	Onze referentie	Bijlage(n)	Datum
	DA230014		20.06.2023

Betreft: Advies betreffende 1) het voorontwerp van wet tot oprichting van de gemeenschappelijke gegevensbank 'Terrorisme, Extremisme, Radicaliseringsproces' ('T.E.R.') en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt en 2) het ontwerp van koninklijk besluit betreffende de gemeenschappelijke gegevensbank 'Terrorisme, Extremisme, Radicaliseringsproces' ('T.E.R.')

Het Controlegeorgaan op de politie-informatie (hierna afgekort 'COC' of 'Controlegeorgaan').

Gelet op de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (BS, 5 september 2018, hierna afgekort als 'WGB') inzonderheid het artikel 59 §1, 2^e lid, artikel 71 en Titel VII, inzonderheid artikel 236.

Gelet op de wet van 3 december 2017 tot oprichting van een Gegevensbeschermingsautoriteit (hierna afgekort 'WOG').

Gelet op de wet van 5 augustus 1992 op het politieambt (hierna 'WPA').

Gelet op de *Law Enforcement Directive* 2016/680 van 27 april 2016 (hierna *LED*).

Gelet op het verzoek van de Minister van Justitie van 14 april 2023 om advies uit te brengen over 1) het voorontwerp van wet tot oprichting van de gemeenschappelijke gegevensbank 'Terrorisme, Extremisme, Radicaliseringsproces' ('T.E.R.') en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt en 2) het ontwerp van koninklijk besluit betreffende de gemeenschappelijke gegevensbank 'Terrorisme, Extremisme, Radicaliseringsproces' ('T.E.R.');

Gelet op het verslag van de heer Koen Gorissen, Lid-raadsheer van het Controlegeorgaan.

Brengt op 20 juni 2023 het volgend advies uit.

I. Voorafgaande opmerking nopens de bevoegdheid van het Controleorgaan

1. In het licht van, respectievelijk, de toepassing en omzetting van de Verordening 2016/679¹ en de Richtlijn 2016/680² heeft de wetgever de taken en opdrachten van het Controleorgaan grondig gewijzigd. Artikel 4 § 2, vierde lid, van de organieke wet van 3 december 2017 betreffende de oprichting van een Gegevensbeschermingsautoriteit (hierna afgekort 'WOG') bepaalt dat de competenties, taken en bevoegdheden als toezichthoudende autoriteit voorzien door de Verordening 2016/679 voor de politiediensten in de zin van artikel 2,2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie, gestructureerd op twee niveaus, worden uitgeoefend door het Controleorgaan. Het betekent onder meer dat het Controleorgaan ook bevoegd is wanneer politiediensten persoonsgegevens verwerken die buiten de opdrachten van bestuurlijke en gerechtelijke politie vallen, bijvoorbeeld in het kader van sociaaleconomische doeleinden of human resources verwerkingen. Het Controleorgaan moet geraadpleegd worden bij de voorbereiding van wetgeving of een regelgevende maatregel die verband houdt met de verwerking van persoonsgegevens door de politiediensten van de geïntegreerde politie (zie artikel 59 §1, 2^e lid en 236 §2 WGB, artikel 36.4 van de AVG en artikel 28.2 van de Richtlijn politie-justitie). Daarbij heeft het Controleorgaan de opdracht om te onderzoeken of de voorgenomen verwerkingsactiviteit door de politiediensten in overeenstemming is met de bepalingen van Titel 1 (voor de niet operationele verwerkingen)³ en 2 (voor de operationele verwerkingen) van de WGB⁴. Daarnaast heeft het COC ook een ambtshalve adviesopdracht voorzien in artikel 236 §2 WGB en een algemene voorlichtingsopdracht van het brede publiek, betrokkenen, verwerkingsverantwoordelijken en verwerkers in de materie van het privacy – en gegevensbeschermingsrecht voorzien in artikel 240 WGB.

2. Wat betreft derhalve in het bijzonder de verwerkingsactiviteiten in kader van de opdrachten van bestuurlijke en/of gerechtelijke politie brengt het Controleorgaan advies uit, hetzij uit eigen beweging, hetzij op verzoek van de Regering of van de Kamer van volksvertegenwoordigers, van een bestuurlijke of gerechtelijke overheid of van een politiedienst, inzake iedere aangelegenheid die betrekking heeft op het politionele informatiebeheer zoals geregeld in Afdeling 12 van Hoofdstuk 4 van de wet op het politieambt⁵.

¹ Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 "betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG" (algemene verordening gegevensbescherming of 'AVG').

² Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 "betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad" (hierna 'Richtlijn Politie en Justitie' of *Law Enforcement Directive (LED)*).

³ Artikel 4 §2, 4^e lid WOG.

⁴ Artikel 71 §1, 3^e lid WGB.

⁵ Artikelen 59 §1, 2^e lid en 236 §2 WGB.

3. Het Controleorgaan is, ten aanzien van de politiediensten, de Algemene Inspectie van de federale politie en lokale politie (afgekort 'AIG') zoals bedoeld in de wet van 15 mei 2007 op de Algemene Inspectie en de Passagiersinformatie-eenheid (hierna afgekort 'BELPIU') bedoeld in Hoofdstuk 7 van de wet van 25 december 2016 tevens belast met het toezicht op de toepassing van Titel 2 van de GBW en/of de verwerking van persoonsgegevens zoals bedoeld in de artikelen 44/1 tot 44/11/13 van de wet op het politieambt en/of elke andere opdracht die haar krachtens of door andere wetten wordt verleend⁶.

4. Het Controleorgaan is ingevolge artikel 281, § 4, van de algemene wet van 18 juli 1977 "*inzake douane en accijnzen*", zoals gewijzigd door de wet van 2 mei 2019 "*tot wijziging van diverse bepalingen met betrekking tot de verwerking van persoonsgegevens*" ten aanzien van de Dienst Geschillen van de Algemene Administratie van Douane en Accijnzen bevoegd in het kader van de vorderingen gericht aan de BELPIU in fiscale materies.

5. Het COC is tot slot ook belast, in het kader van de dataretentie wetgeving, op grond van artikel 126/3 §1, 8^e lid van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna afgekort 'WEC'), zoals gewijzigd door de wet van 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten (*BS* van 8 augustus 2022), met de validatie van de statistieken met betrekking tot het aantal strafbare feiten en de bewaringstermijn voor elk gerechtelijk arrondissement en elke politiezone in het kader waarvan het al zijn bevoegdheden uitoefent die hem zijn toegekend bij titel 7 van de wet van 30 juli 2018. Het is daarnaast ook nog belast, in toepassing van artikel 42 § 3, 2^{de} en 3^{de} lid WPA met de controle van de vorderingen van de Cel Vermiste Personen van de federale politie tot opvraging van de gegevens met betrekking tot de elektronische communicatie betreffende de vermiste persoon.

6. Het Controleorgaan is bevoegd om advies te verlenen over aspecten met betrekking tot de verwerking van informatie en persoonsgegevens en de bescherming van het privéleven door de verwerking van persoonsgegevens voor zover deze betrekking hebben op of in verband staan met de operationele en niet-operationele werking van de politiediensten en/of het personeel van de geïntegreerde politie (hierna 'GPI'⁷) en/of voor zover de voor advies voorgelegde ontwerp tekst een impact heeft op de politieke informatiehuishouding in het algemeen.

⁶ Artikel 71 §1, derde lid *juncto* 236 § 3 WGB.

⁷ Geïntegreerde politie – Police Intégrée.

7. Het Controleorgaan is daarnaast niet enkel een gegevensbeschermingsautoriteit maar een toezichthouder die evenzeer wettelijk belast is met de legaliteit, efficiëntie, effectiviteit en economie van de politionele informatiehuishouding⁸.

II. Voorwerp van de aanvraag

8. De adviesaanvraag heeft betrekking op 1) het voorontwerp van wet tot oprichting van de gemeenschappelijke gegevensbank 'Terrorisme, Extremisme, Radicaliseringsproces' ('T.E.R.') en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme en de wet van 5 augustus 1992 op het politieambt (hierna 'het wetsontwerp T.E.R.') en 2) het ontwerp van koninklijk besluit betreffende de gemeenschappelijke gegevensbank 'Terrorisme, Extremisme, Radicaliseringsproces' ('T.E.R.') (hierna 'het ontwerp KB T.E.R.'). Aangezien beide teksten nauw verbonden zijn, worden ze samen in dit advies behandeld.

9. Het wetsontwerp T.E.R. strekt overeenkomstig de Memorie van toelichting (MvT) tot de opname in een autonome wet van de bepalingen van de WPA met betrekking tot de gemeenschappelijke gegevensbanken 'Terrorist Fighters' en 'Haatpropagandisten', waarvan de verwerkingsmodaliteiten worden uiteengezet in het KB van 21 juli 2016 "*betreffende de gemeenschappelijke gegevensbank Terrorist Fighters*" en in het KB van 23 april 2018 "*betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1bis "Het Informatiebeheer" van hoofdstuk IV van de wet op het politieambt*".

Volgens de MvT kunnen op deze manier een aantal regels gestroomlijnd worden, door de gemeenschappelijke gegevensbanken 'Terrorist Fighters' en 'Haatpropagandisten' samen te voegen in éénzelfde juridisch instrument. Ook werden processen herschreven, definities toegevoegd of herschreven, doeleinden aangepast en heel wat essentieel geachte bepalingen uit de Koninklijke besluiten vastgelegd in dit wetsontwerp. In het ontwerp worden verder nog bepalingen toegevoegd inzake de bescherming van persoonsgegevens, wordt voorzien in een systematisch overleg voor de opvolging van de entiteiten en worden het bestaan en de opdrachten van de lokale Taskforces (LTF) bekrachtigd en vastgelegd.

10. De oprichting van een autonome wet voor de gemeenschappelijke gegevensbank inzake terrorisme, extremisme of het radicaliseringsproces wordt overeenkomstig de MvT gemotiveerd met de volgende redenen :

⁸ Activiteitenverslag 2021, www.controleorgaan.be, randnummers 3, 52 en in het bijzonder 71: "*Het COC heeft echter allerm minst alleen oog voor dataprotectie; het heeft evenzeer veel aandacht en is bevoegd voor alle andere operationele aspecten van de politionele informatiehuishouding*"; artikel 71 §1 WGB.

- gehoor geven aan zowel de parlementaire onderzoekscommissie als de GBA om een *ad hoc* rechtsgrondslag te geven aan deze gegevensbank, die geen specifieke reden had om aan de WPA gekoppeld te zijn;
- de noodzaak om na de 'zaak Conings' de lokale Taskforce te verplichten om een lijst maatregelen te overlopen die ten aanzien van een entiteit kunnen worden genomen;
- de noodzaak om de basisdiensten de mogelijkheid te bieden bepaalde gegevens van T.E.R. entiteiten mee te delen aan zorgverleners, dit naar aanleiding van het tragische overlijden van een politieambtenaar.

De meeste bestaande en in voegde zijnde artikelen van de WPA of de Koninklijke besluiten 'TF' en 'HP' zijn in het wetsontwerp overgebracht zonder inhoudelijke wijziging. Enkel de nieuwe bepalingen worden in de MvT uiteengezet en toegelicht, voor het overige wordt verwezen naar de parlementaire werkzaamheden van de wet van 27 april 2016 inzake aanvullende maatregelen ter bestrijding van terrorisme en naar de verslagen aan de Koning van de voornoemde Koninklijke uitvoeringsbesluiten.

Het ontwerp KB T.E.R. tenslotte heeft, overeenkomstig het verslag aan de Koning, tot doel om bepaalde aspecten van de gemeenschappelijke gegevensbank T.E.R., opgericht door het wetsontwerp T.E.R., uit te werken.

Aangezien beide ontwerpen een impact hebben op het informatiebeheer door de GPI, zal het Controleorgaan zich in dit advies beperken tot de aspecten van het ontwerp die daarmee in verband staan. Voor het overige verwijst het controleorgaan naar het advies van de GBA en naar zijn eerdere adviezen en rapporten⁹ met betrekking tot de gemeenschappelijke gegevensbanken TF en Haatpredikers.

III. Bespreking en analyse van de aanvraag

A. Algemeen

11. Het Controleorgaan verwelkomt de omzetting in een autonome wet van de bepalingen in de WPA met betrekking tot de gemeenschappelijke gegevensbanken 'Terrorist Fighters' en 'Haatpropagandisten'. Deze *ad hoc* rechtsgrondslag vormt een logische keuze voor dergelijke, voor verschillende diensten(gemeenschappelijke) toegankelijke gegevensbanken, die niet noodzakelijk en zelfs beter niet in de WPA dienden te worden opgenomen, vermits het niet gaat om een zuivere politionele gegevensbank (zoals alle andere, met name de basisgegevensbanken, de ANG, de bijzondere gegevensbanken en de technische gegevensbanken). Vervolgens wordt, door de creatie

⁹ Zie de gezamenlijke rapporten van het Controleorgaan op de politionele informatie en het Vast Comité I inzake de gemeenschappelijke gegevensbanken TF, uitgebracht in de jaren 2017, 2018, 2019 en 2020, evenals de adviezen inzake de voorafgaandelijke aangiften van de gemeenschappelijke gegevensbanken TF (niet gepubliceerd).

van deze autonome wet en de opname van de belangrijkste elementen van de uitvoerings KB's in deze wet, een sterkere juridische grondslag gecreëerd.

12. Het Controleorgaan stelt ook vast dat de steller van het ontwerp van deze gelegenheid heeft gebruik gemaakt om bepaalde aspecten van de bestaande regelgeving tegen het licht te houden en de noodzakelijkheid ervan te evalueren. Zo werden bepaalde vroegere partnerdiensten niet meer in de actuele lijst van partnerdiensten in het wetsontwerp opgenomen, gezien hun gebrek aan een 'behoefte om te kennen'. In hun gezamenlijke rapporten van 2018 en 2019 inzake de gemeenschappelijke gegevensbanken TF (GGB TF) hadden het COC en Vast Comité I reeds op de problematiek van de herziening van de toegang van bepaalde partnerdiensten gewezen, gelet op het gebrek van een 'behoefte om te kennen', en dit onder meer omdat voor meerdere jaren geen enkele gebruiker werd (wordt) aangeduid die toegang tot de GGB TF kon (kan) nemen.

13. Het specifieke type van toegang (creatierecht, leesrecht, schrijfrecht, vraagrecht¹⁰) van de respectievelijke partnerdiensten wordt niet in het wetsontwerp geregeld, maar overgelaten aan de Koning. **Het verdient echter aanbeveling om het specifieke type van toegang tot de gemeenschappelijke gegevensbank, alsook het kader waarin de betreffende partnerdienst die rechten zal mogen aanwenden, in het wetsontwerp zelf te voorzien. Het betreft namelijk een essentieel element van de verwerking van persoonsgegevens¹¹.**

Aangezien de meeste artikelen uit de WPA of de Koninklijke besluiten TF in het wetsontwerp en/of het ontwerp KB zijn overgebracht zonder inhoudelijke wijziging, zal het Controleorgaan hiernavolgend in het bijzonder de nieuwe of ingrijpend gewijzigde artikelen analyseren, die in het bijzonder een impact hebben op het informatiebeheer door de GPI.

B. Artikelsgewijze bespreking Wetsontwerp T.E.R.

14. Artikel 6, §2, 2° van het wetsontwerp bepaalt dat de in de gemeenschappelijke gegevensbank T.E.R. verwerkte persoonsgegevens zijn : " ... *de administratieve gegevens, de gerechtelijke gegevens,*

¹⁰ Zie artikel 2 van het wetsontwerp, 11°-14°;

¹¹ Recent nog oordeelde het Grondwettelijk Hof bij arrest van 10 maart 2022 (GwH, n° 33/2022 van 10 maart 2022, overweging, B.13.1, www.grondwettelijkhof.be) hieromtrent als volgt: "Bij artikel 22 van de Grondwet wordt aan de bevoegde wetgever de bevoegdheid voorbehouden om te bepalen in welke gevallen en onder welke voorwaarden afbreuk kan worden gedaan aan het recht op eerbiediging van het privéleven. Het waarborgt aldus aan elke burger dat geen inmenging in de uitoefening van dat recht kan plaatsvinden dan krachtens regels die zijn aangenomen door een democratisch verkozen beraadslagende vergadering.

...

Bijgevolg moeten de essentiële elementen van de verwerking van persoonsgegevens in de wet zelf worden vastgelegd¹¹. In dat verband maken de volgende elementen, ongeacht de aard van de betrokken aangelegenheid, in beginsel essentiële elementen uit : 1°) de categorie van verwerkte gegevens; 2°) de categorie van betrokken personen; 3°) de met de verwerking nagestreefde doelstelling; 4°) de categorie van personen die toegang hebben tot de verwerkte gegevens en 5°) de maximumtermijn voor het bewaren van de gegevens (advies van de algemene vergadering van de afdeling wetgeving van de Raad van State nr. 68.936/AV van 7 april 2021 over een voorontwerp van wet « betreffende de maatregelen van bestuurlijke politie tijdens een epidemische noodsituatie », Parl. St., Kamer, 2020-2021, DOC 55-1951/001, p. 119)" (overweging B.13.1)

de gegevens van gerechtelijke politie, de gegevens van bestuurlijke politie en de informatie betreffende de geregistreerde entiteiten, die overeenkomstig de wet verwerkt worden door de basisdiensten, waaronder de GPI, en de partnerdiensten die een leesrecht en een schrijfrecht hebben in de gemeenschappelijke gegevensbank T.E.R. en die toereikend, ter zake dienend en niet overmatig zijn in het licht van de opdrachten bedoeld in artikel 3 en de doeleinden bedoeld in artikel 5, tweede lid."

Voor de GPI gaat het derhalve over gegevens van gerechtelijke en bestuurlijke politie, weliswaar enkel na evaluatie of deze toereikend, ter zake dienend en niet overmatig zijn in het licht van de opdrachten en de doeleinden van het wetsontwerp, zoals de MvT ook benadrukt. Als basisdienst beschikt de GPI over een creatierecht van een entiteit in de GGB T.E.R., en zal ze derhalve bij de creatie rekening dienen te houden met deze elementen. De nadere regels voor het creatierecht worden overeenkomstig artikel 18 van het wetsontwerp nader uitgewerkt door de Koning (hiervoor in het bijzonder artikel 14 van het ontwerp KB met betrekking tot de interne validatie). Een voormelde evaluatie in het licht van de opdrachten en de doeleinden van het wetsontwerp zal bij de interne validatie dan ook moeten worden opgenomen, temeer aangezien er geen beperking staat op de aard van de politionele informatie die kan worden overgemaakt aan de GGB T.E.R. .

Gegevens van bestuurlijke en gerechtelijke politie maakt namelijk een zeer ruime en diverse categorie van (persoons)gegevens uit: het betekent de facto dat zowat de hele 'ANG bestuurlijk en gerechtelijk' voorwerp kunnen vormen van een opname in de GGB, alsook dat alle mogelijke informatie en persoonsgegevens uit de basisgegevensbanken, de bijzondere gegevensbanken en de technische gegevensbanken kunnen opgenomen worden. Er wordt in het wetsontwerp op geen enkele wijze rekening gehouden met de validatiestatus van de politionele persoonsgegevens en informatie. Ook ruwe of brute informatie – die geen validatieproces heeft doorlopen - zoals die in de basisgegevensbanken worden gevat, maken of kunnen het voorwerp uitmaken van een opname in de GGB T.E.R.. Zowel harde (processen-verbaal) als zachte informatie (in informatierapporten, niet concrete feiten m.a.w.) kunnen eveneens het voorwerp ervan uitmaken. Indien dit niet het geval zou zijn, komt het aan de steller van het ontwerp toe om dit nader te verduidelijken in het wetsontwerp.

15. In het belang van de betrokken persoon en van de zorgverlener, deelt de basisdienst (waaronder de GPI) die met laatstgenoemde in contact staat, hem conform het ontworpen art. 6 §2, 3°, 2^e lid van het wetsontwerp de nodige medische gegevens mee die geregistreerd zijn in de GGB T.E.R. alsook de gegevens die afkomstig zijn van de dreigingsevaluatie met betrekking tot het gevaar dat uitgaat van de betrokken persoon. **Het verdient aanbeveling om deze communicatie vanuit de GPI schriftelijk vast te leggen, teneinde eventueel achteraf discussie te vermijden. Zie hieromtrent tevens infra, randnummer 24.**

16. Artikel 7 bepaalt dat, na de laatste verwerking, de operationeel verantwoordelijke om de vijf jaar (of om de drie jaren ingeval van minderjarigen) onderzoekt of de persoonsgegevens nog steeds een rechtstreeks verband vertonen met een van de doeleinden van artikel 5 van het wetsontwerp. Indien dit niet het geval is, worden de gegevens gearhiveerd. Het wetsontwerp voorziet in een maximale archiveringstermijn van 30 jaren, naar analogie met hetgeen de WPA¹² voorziet. Een dergelijke bijkomende bewaringstermijn via archivering, van maximaal 30 jaren, lijkt moeilijk houdbaar in het licht van recente rechtspraak¹³ van het Europees Hof van Justitie, en de principes uit het gegevensbeschermingsrecht ('proportioneel, ter zake dienend en niet overmatig'), zoals trouwens beschreven in het wetsontwerp. Het lijkt dan ook een contradictie om de gegevens, indien er geen verband meer is met één van de doeleinden van artikel 5 van het wetsontwerp, te archiveren, in plaats van deze te wissen wegens niet meer proportioneel, ter zake dienend en overmatig. **Het komt de steller van het ontwerp dan ook toe om zich hieromtrent te beraden, en minstens een kritische toetsing te doen van het beoogde archiveringssysteem, dat een kopie uitmaakt van hetgeen is voorzien in de WPA.**

In hun verslagen van de gezamenlijke controle van de GGB TF hebben het Controleorgaan en het Vast Comité I tevens herhaaldelijk gewezen op de noodzaak van de strikte opvolging van deze termijnen, en dit via de ontwikkeling van een ICT Tool. Het moet voor de toezichthoudende overheden (COC en Vast Comité I) immers mogelijk zijn om de correcte naleving van deze termijn na te gaan. **Het verdient derhalve aanbeveling om in het wetsontwerp op te nemen dat de operationeel verantwoordelijke deze evaluatie opneemt in het dossier van de betreffende entiteit, opdat een verificatie van de evaluatie en de termijn door de toezichthoudende overheden mogelijk is, evenals een strikte opvolging van deze termijnen aan de hand van een ICT applicatie.**

17. Artikel 9 van het wetsontwerp voorziet in de mogelijkheid tot koppeling van de GGB T.E.R. met andere gegevensbanken die worden beheerd door de basis -of partnerdiensten. Dergelijke koppeling houdt overeenkomstig de definitie in artikel 2, 16° van het wetsontwerp onder meer in dat persoonsgegevens en relevante informatie van de gegevensbanken, authentieke bronnen, kunnen worden overgezonden aan de GGB T.E.R.

Voor de GPI betekent dat bijvoorbeeld een koppeling met de ANG en alle andere politionele gegevensbanken. De vraag stelt zich naar de verhouding tussen dit artikel van het wetsontwerp en de bepalingen van de artikelen 44/11/4 en volgende van de WPA. **Het komt de steller van het ontwerp toe om hieromtrent duiding te verschaffen.**

¹² Zie bijvoorbeeld artikel 44/10 van de wet op het politieambt, voor wat betreft de archivering van persoonsgegevens en informatie in de ANG.

¹³ HvJ EU 21 juni 2022, Zaak C-817/19.

Verder bepaalt artikel 9 dat de Koning in voormelde gevallen de doeleinden van de koppeling bepaalt, de onderling verbonden categorieën van persoonsgegevens en de nadere regels van de koppeling, waarbij de integriteit van de gegevens en van de netwerken gerespecteerd moeten worden. **In deze dient te worden voorzien in het voorafgaand advies van de toezichthoudende overheden aangaande voormeld Koninklijk besluit, waaronder het Controleorgaan, als bevoegde toezichthoudende autoriteit van de politiediensten, zoals bedoeld in artikel 26, 7°, a) WGB.**

18. Artikel 17 regelt de mogelijke toegangsrechten (leesrecht, schrijfrecht of vraagrecht) voor de partnerdiensten, maar laat de uitwerking ervan over aan de Koning. De MvT verklaart deze keuze voor een KB teneinde een zekere flexibiliteit te behouden bij het verlenen, intrekken of wijzigen van de toegang naar gelang van de evolutie van de bevoegdheden, opdrachten en behoeften van de verschillende partnerdiensten. **Zoals het COC reeds heeft opgemerkt onder randnummer 13, verdient het echter aanbeveling om het specifieke type van toegang tot de gemeenschappelijke gegevensbank, alsook het kader waarin de betreffende partnerdienst die rechten zal mogen aanwenden, in het wetsontwerp te voorzien. De GGB TF en HP zijn inmiddels reeds ettelijke jaren operationeel, waardoor men alleszins de noden voor de respectievelijke opdrachten en behoeften van de verschillende partnerdiensten behoort te kennen.**

19. Overeenkomstig artikel 19 van het wetsontwerp wordt voorzien dat de basisdiensten, waaronder de GPI, verplicht zijn respectievelijk de GGB T.E.R. te raadplegen en ambtshalve hun eigen persoonsgegevens en relevante informatie daarin te voeren. Die gegevens worden onder hun verantwoordelijkheid en overeenkomstig hun interne validatieprocedures opgenomen in de GGB. Deze persoonsgegevens en informatie worden afgeleid uit de persoonsgegevens en informatie waarover de basisdiensten beschikken in het kader van hun respectieve opdrachten en de daarmee verband houdende doeleinden. **Hieromtrent kan verwezen worden naar de gemaakte opmerkingen onder randnummer 14.**

Het 4^{de} lid van artikel 19 bepaalt verder dat de GPI de persoonsgegevens en informatie invoeren overeenkomstig de aanvullende specificaties in de richtlijn van het College van PG. Daarnaast bepaalt artikel 20 dat het creatie -en schrijfrecht in de GGB T.E.R. worden uitgesteld wanneer en zolang de bevoegde magistraat, meent dat de creatie en de voeding de uitoefening van de strafvordering, de veiligheid van een persoon of de relatie met de rechtshandavingsinstantie van een Buitenlandse staat in het gedrang kunnen brengen. In hun eerdere rapporten met betrekking tot de GGB TF hebben het COC en het Vast Comité I gewezen op het feit dat politionele informatie afkomstig van "RIR, codes 01 of 00", niet wordt opgenomen in de GGB. Een "RIR 01" heeft betrekking op politionele informatie die enkel mag worden gebruikt voor zover de opsteller daarmee akkoord gaat. Een "RIR 00" heeft betrekking op politionele informatie die in geen geval mag worden gebruikt. Het betreft gevoelige

informatie (die echter niet werd geclassificeerd) die, bijvoorbeeld, kan leiden tot de identificatie van een bron. Deze codes zijn het resultaat van een ministeriële omzendbrief die slechts ten dele en zeer beperkt werd gepubliceerd, i.e. omzendbrief "MFO 3", betreffende – onder andere – de gegevensinvoer in de Algemene Nationale Gegevensbank (ANG) van de Geïntegreerde Politie.

De regelgeving voorziet niet in uitzonderingen wat betreft de doorgifte van dit soort politionele informatie naar de GGB. Deze informatie zou dus verplichtend moeten worden opgenomen in de GGB. Vanuit juridisch oogpunt immers hebben (in het verleden) de WPA en (in de toekomst) het wetsontwerp T.E.R. en de uitvoeringsbesluiten voorrang op de omzendbrief MFO 3, krachtens het beginsel van de hiërarchie der normen (de MFO 3 wordt immers gebaseerd op de bepalingen van het informatiebeheer van de WPA). De voorbije jaren hebben het C.O.C. en het Vast Comité I dus aanbevolen om deze problematiek te evalueren en deze situatie te verhelpen. **Het komt de steller van het ontwerp dan ook toe om dit te regelen in huidig wetsontwerp, dan wel hieromtrent minstens duidelijkheid te verschaffen bijvoorbeeld in de MvT.**

20. Artikel 22 van het wetsontwerp voorziet de informatie aan de bevoegde bestuurlijke overheden door de korpschef van elke betrokken politiezone ingeval van de creatie van een nieuwe entiteit in de GGB T.E.R. Betreft het hier eveneens een nieuwe entiteit overeenkomstig artikel 2, 6° van het ontwerp KB waarover ernstige aanwijzingen bestaan dat zij de criteria bedoeld in artikel 1, 4°, 5°, 6°, of 8° van het ontwerp KB T.E.R. kunnen vervullen ? indien dit niet het geval is, dienen deze entiteiten immers na zes maanden te worden gearchiveerd overeenkomstig artikel 13 van het ontwerp KB T.E.R. Vallen hier met andere woorden dus ook de 'proef of potentiële entiteiten' onder ? Het zou immers kunnen dat na enkele maanden blijkt dat een dergelijke 'proef of potentiële entiteit' niet in de GGB T.E.R. kan worden opgenomen. **Het verdient aanbeveling om hieromtrent duidelijkheid te verschaffen. Voor zover hieronder ook voormelde categorie van entiteiten valt die blijken na zes maanden niet te worden gevalideerd als entiteit dient ook die informatie van niet bevestiging aan voormelde bestuurlijke overheden te worden kenbaar gemaakt en dient er zorg te worden voor gedragen dat deze informatie bij die bestuurlijke entiteit wordt gewist.**

21. Overeenkomstig artikel 24 van het wetsontwerp kan een informatiekaart worden meegedeeld aan een derde overheid die de behoefte om te kennen heeft, na evaluatie door de beheerder, de operationeel verantwoordelijke en de basisdiensten. Dergelijke evaluatie heeft minstens betrekking op 4 elementen, zijnde 1) de bijdrage van de derde overheid tot de preventie en bestrijding van terrorisme en extremisme dat tot terrorisme kan leiden 2) de verdere verwerking die zal worden gedaan door de derde overheid rekening houdende met haar bevoegdheden en de eventuele risico's voor de fundamentele vrijheden en rechten van de betrokken persoon 3) de kwetsbare toestand van de betrokken persoon, inclusief de minderjarigheid; 4) het toereikende, ter zake dienend en niet overmatige karakter van de categorieën van meegedeelde gegevens rekening houdend met de verdere

verwerking. Ook inzake deze doorgifte van lijsten hebben het COC en het Vast Comité I in het verleden opmerkingen gemaakt aangaande de wettelijkheid van deze doorgifte. Het COC verwelkomt dan ook de regeling in het wetsontwerp, in het bijzonder de minimale criteria voor evaluatie van een dergelijke doorgifte. **Teneinde een doeltreffende controle hierop mogelijk te maken, wordt de steller van het ontwerp verzocht om uitdrukkelijk te voorzien dat door de operationeel verantwoordelijke, ten behoeve van de toezichthoudende overheden, een lijst van dergelijke mededelingen aan derde overheden wordt bijgehouden, met de mogelijkheid om voor elke doorgifte de opgemaakte evaluatie desbetreffend terug te vinden.**

22. Overeenkomstig artikel 28, §2 van het wetsontwerp kunnen de persoonsgegevens en de informatie uit de GGB T.E.R. in overeenstemming met artikel 44/11/13 WPA aan buitenlandse politiediensten, buitenlandse gerechtelijke autoriteiten en internationale organisaties voor gerechtelijke en politionele samenwerking worden overgemaakt. In §4 wordt verder bepaald dat de Koning nadere regels voor deze mededeling kan bepalen. **Ook hier dient te worden voorzien in het voorafgaand advies van de toezichthoudende overheden op voormeld Koninklijk besluit, waaronder het Controleorgaan, als bevoegde toezichthoudende autoriteit van de politiediensten, zoals bedoeld in artikel 26, 7°, a) WGB.**

23. Artikel 30 voorziet dat de verantwoordelijkheid voor de kwaliteit van de persoonsgegevens, en de informatie die geregistreerd zijn in de GGB T.E.R., toekomt aan de verwerkingsverantwoordelijke eigen aan elke dienst die de GGB T.E.R. voedt. Dit betekent voor de GPI, in het bijzonder voor de ANG en de basisgegevensbanken, dat de ministers van Justitie en Binnenlandse zaken optreden als verwerkingsverantwoordelijken. Zij zijn echter eveneens verwerkingsverantwoordelijke voor de GGB T.E.R. zelf overeenkomstig artikel 5 van het wetsontwerp.

Het begrip “verwerkingsverantwoordelijke” is evenwel een functioneel begrip dat als doel heeft de verantwoordelijkheden toe te kennen aan de personen die feitelijke invloed uitoefenen¹⁴. Concreet betekent dit dat de entiteit die beslist over het ‘hoe’ en het ‘wat’ van de gegevensverwerking de verwerkingsverantwoordelijke zal zijn, los van het statuut, de positie of de situatie dat/die wordt toegekend aan deze entiteit binnen haar organisatie. De bevoegdheid om te ‘bepalen’ kan weliswaar worden geregeld via de wet, maar blijkt tevens uit de bevoegdheden die zijn toegewezen aan een bepaalde entiteit of ook uit een analyse van de feiten en de omstandigheden.

In deze zin beschouwt het Controleorgaan – en het handelt dienovereenkomstig in de praktijk – de politiediensten, op het federale en het lokale niveau, als de “operationele verwerkingsverantwoordelijke”, daar zij een doorslaggevende feitelijke invloed en impact hebben op

¹⁴ Werkgroep “Artikel 29” inzake gegevensbescherming, Advies 1/2010 over de begrippen ‘verwerkingsverantwoordelijke’ en ‘verwerker’, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_fr.pdf, p. 12.

de concrete en effectieve verwerking (registratie) van de persoonsgegevens en ze daar meester van zijn.

Het Controleorgaan is vragende partij¹⁵ voor de omzetting van deze werkelijkheid op het terrein in de wet op het politieambt. Een doeltreffende controle door het COC en een correcte wetgeving inzake de bescherming van politiegegevens vereisen, inzake juridische duidelijkheid, dat de operationele verwerkingsverantwoordelijke als zodanig wordt gedefinieerd door de wet.

Het is derhalve aangewezen om in artikel 30 van het wetsontwerp voor de GPI te werken met zogenaamde 'operationele verwerkingsverantwoordelijken', die daadwerkelijk instaan voor de voeding van de GGB T.E.R., en derhalve ook het best geplaatst zijn om in te staan voor de kwaliteit van de persoonsgegevens en informatie.

24. Tenslotte voorziet artikel 53 van het wetsontwerp in de invoeging van een artikel 44/11/9 *bis* in de WPA, aangaande de uitwisseling van persoonsgegevens en informatie door de GPI aan gezondheids-, hulp- en/of reddingsdiensten. **Zoals reeds vermeld onder randnummer 15, verdient het aanbeveling om tevens op te nemen dat deze communicatie vanuit de (GPI) wordt geregistreerd, teneinde eventueel achteraf discussie te vermijden.**

25. Het wetsontwerp T.E.R. geeft voor het overige geen aanleiding tot andere opmerkingen vanwege het Controleorgaan.

C. Artikelsgewijze bespreking ontwerp KB T.E.R.

26. Artikel 2, 6° van het ontwerp KB vermeldt als categorie van entiteit die in de GGB T.E.R. verwerkt worden *"de identificatiegegevens met betrekking tot de entiteiten ten aanzien van wie er ernstige aanwijzingen bestaan dat zij de criteria bedoeld in artikel 1, 4°, 5°, 6° of 8° kunnen vervullen"*. Artikel 13 van het ontwerp KB voorziet dat deze gegevens maximaal zes maanden mogen worden bewaard vanaf de registratiedatum, en op het einde van de termijn worden gearhiveerd indien zij niet beantwoorden aan de voormelde criteria van artikel 1. **De steller van het ontwerp wordt dan ook verzocht om deze bewaartermijn eveneens in het wetsontwerp zelf te voorzien, en niet in het ontwerp KB. Het betreft namelijk een essentieel element van de verwerking van persoonsgegevens.**

In hun verslagen van de gezamenlijke controle van de GGB TF hebben het Controleorgaan en het Vast Comité I herhaaldelijk gewezen op de noodzaak van de strikte opvolging van deze termijnen, en dit

¹⁵ Zie ook de adviezen in de dossiers DA220017 (SIS) en DA220030 (DPO), te consulteren op de website van het Controleorgaan : <https://www.controleorgaan.be/nl/publicaties>

via de ontwikkeling van een ICT Tool. Het moet niet enkel voor de operationele verantwoordelijke, maar ook voor de toezichthoudende overheden (COC en Vast Comité I) immers mogelijk zijn om de correcte naleving van deze termijn na te gaan. **De steller van het ontwerp wordt dan ook verzocht om in het ontwerp KB op te nemen dat de operationeel verantwoordelijke deze evaluatie opneemt in het dossier van de betreffende entiteit, opdat een verificatie van de evaluatie en de termijn door de toezichthoudende overheden mogelijk is, evenals een strikte opvolging van deze termijnen aan de hand van een ICT applicatie.**

OM DEZE REDENEN

Het Controleorgaan op de Politie Informatie,

verzoekt de aanvrager rekening te houden met de hogervermelde opmerkingen.

Advies goedgekeurd door het Controleorgaan op de Politie Informatie op 20 juni 2023.

Voor het Controleorgaan,
De Voorzitter a.i.,
(GET) Frank Schuermans