DOC 54 **3697/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

27 maart 2019

WETSVOORSTEL

tot wijziging van diverse bepalingen wat het politionele informatiebeheer betreft

(ingediend door de heer Franky Demon en de dames Veerle Heeren, Katja Gabriëls en Sandrine De Crom)

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

27 mars 2019

PROPOSITION DE LOI

modifiant diverses dispositions en ce qui concerne la gestion de l'information policière

(déposée par M. Franky Demon et Mmes Veerle Heeren, Katja Gabriëls et Sandrine De Crom)

N-VA	:	*Nieuw-Vlaamse Alliantie*
PS	:	*Parti Socialiste*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
Open Vld	:	*Open Vlaamse liberalen en democraten*
sp.a	:	*socialistische partij anders*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
cdH	:	*centre démocrate Humaniste*
VB	:	*Vlaams Belang*
PTB-GO!	:	*Parti du Travail de Belgique – Gauche d'Ouverture*
DéFI	:	*Démocrate Fédéraliste Indépendant*
PP	:	*Parti Populaire*
Vuye&Wouters	:	*Vuye&Wouters*

Afkortingen bij de nummering van de publicaties:

DOC 54 0000/000:	*Parlementair document van de 54e zittingsperiode + basisnummer en volgnummer*
QRVA:	*Schriftelijke Vragen en Antwoorden*
CRIV:	*Voorlopige versie van het Integraal Verslag*
CRABV:	*Beknopt Verslag*
CRIV:	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*
PLEN:	*Plenum*
COM:	*Commissievergadering*
MOT:	*Moties tot besluit van interpellaties (beigekleurig papier)*

Abréviations dans la numérotation des publications:

DOC 54 0000/000:	*Document parlementaire de la 54e législature, suivi du n° de base et du n° consécutif*
QRVA:	*Questions et Réponses écrites*
CRIV:	*Version Provisoire du Compte Rendu intégral*
CRABV:	*Compte Rendu Analytique*
CRIV:	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN:	*Séance plénière*
COM:	*Réunion de commission*
MOT:	*Motions déposées en conclusion d'interpellations (papier beige)*

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers

Bestellingen:
Natieplein 2
1008 Brussel
Tel. : 02/ 549 81 60
Fax : 02/549 82 74
www.dekamer.be
e-mail : publicaties@dekamer.be

De publicaties worden uitsluitend gedrukt op FSC gecertificeerd papier

Publications officielles éditées par la Chambre des représentants

Commandes:
Place de la Nation 2
1008 Bruxelles
Tél. : 02/ 549 81 60
Fax : 02/549 82 74
www.lachambre.be
courriel : publications@lachambre.be

Les publications sont imprimées exclusivement sur du papier certifié FSC

SAMENVATTING

Dit voorstel heeft als voorwerp de wetgeving inzake het beheer van persoonsgegevens en van informatie door de politiediensten aan te passen ingevolge de om te zetten Richtlijn 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 overheden 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"). Tevens zijn er enkele wettelijke aanpassingen noodzakelijk krachtens de Verordening 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") die met ingang van 25 mei 2018 van toepassing is (artikel 25.2 AVG).

Bijkomende aanpassingen hebben betrekking op de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (hierna "wet gegevensbescherming"), die in titel 2 de Richtlijn heeft omgezet naar Belgisch recht en bij de Kamer van volksvertegenwoordigers een onafhankelijke toezichthoudende autoriteit op de politionele informatie heeft opgericht, genaamd "Controleorgaan op de politionele informatie" (hierna "Controleorgaan"). In het verlengde hiervan zijn er aanpassingen nodig van de WPA en WGP.

Daarnaast werd, in het belang van de geïntegreerde werking van de politie, ervoor geopteerd om ook te voorzien in de oprichting van een Strategisch adviescomité voor informatie (hierna "Strategisch Comité I"), evenals in een uniek register van de verwerkingsactiviteiten voor de Geïntegreerde Politie.

Aanvullend was het in de huidige realiteit van diverse samenwerkingsvormen tussen de verschillende politiediensten (zoals fusies, associaties, gezamenlijke projecten als Kanaalplan en Stroomplan, ...) en de toekomstige IT-ontwikkelingen die deze vormen van samenwerking ondersteunen (zoals i-Police) ook noodzakelijk om het kader inzake de koppeling van de diverse gegevensbanken verder te specificeren.

RÉSUMÉ

Cette proposition vise à adapter la législation relative à la gestion des données à caractère personnel et des informations par les services de police pour tenir compte de la directive 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 "Directive"), qui doit être transposée. Un certain nombre de modifications légales sont en outre nécessaires en vertu du Règlement 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"), qui est d'application depuis le 25 mai 2018 (article 25.2 RGPD).

Des modifications complémentaires concernent 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 "loi cadre relative à la protection des données"), qui a transposé le titre 2 de la Directive en droit belge et a créé auprès de la Chambre des représentants une autorité indépendante de contrôle de l'information policière dénommée "Organe de contrôle de l'information policière" (ci-après "Organe de contrôle"). Des adaptations doivent dès lors être apportées à la LFP et la LPI.

En plus, il a été décidé de créer, dans l'intérêt du fonctionnement intégré de la police, un Comité d'avis en charge de la stratégie en matière d'information (ci-après "Comité stratégique I"), et un registre des activités de traitement unique pour la Police Intégrée.

Il s'avère en outre nécessaire, dans la réalité actuelle des diverses formes de coopération entre les différents services de police (fusions, associations, projets conjoints tels que Kanaalplan et Stroomplan, ...) et les futurs développements informatiques qui appuient ces formes de coopération (tel que i-Police), de préciser davantage le cadre régissant l'interconnexion des différentes banques de données.

Ook de rechtstreekse toegang van de Inlichtingendiensten tot de Algemene Nationale Gegevensbank (ANG) werd in de wet geschreven. Immers, de Parlementaire Onderzoekscommissie blijft het belang onderschrijven van een betere toegang tot informatie voor deze diensten, en het bestaande concept van rechtstreekse bevraging van de ANG (HIT/NO HIT met bijkomende informatie in geval van een HIT) voldoet niet aan de behoeften of het werkproces van de inlichtingendiensten die moeten kunnen beschikken over het geheel van beschikbare informatie om in de grootst mogelijke discretie onderzoekswerk te kunnen verrichten dat er op gericht is te bepalen of een persoon al dan niet een risico uitmaakt op het vlak van terrorisme of radicalisme. Het spreekt voor zich dat de inlichtingendiensten na dit inlichtingenonderzoek in ruil relevante en verrijkte informatie aanleveren aan de politiediensten op basis van het principe van need to share.

Uiteraard moeten de modaliteiten van deze wederkerigheid met alle relevante partners worden besproken zodat de politie optimaal kan beschikken over de informatie van de inlichtingendiensten die zij nodig heeft om haar taken uit te voeren.

Ten slotte werden de opdrachten van bestuurlijke politie die het gebruik van een technische gegevensbank rechtvaardigen uitgebreid met de categorie van personen die het voorwerp uitmaken van een politiemaatregel. Deze toevoeging werd gedaan ten gevolge van de operationele behoefte van de politiediensten om ANPR-camera's te kunnen inzetten bij de effectieve opvolging van een politiemaatregel, bevolen door een bevoegde overheid, zoals een plaats- of doorgangsverbod.

L'accès direct à la Banque de Données nationale Générale a également été inscrit au profit des services de renseignement. Bien entendu, la CEP continue à souligner l'importance d'améliorer l'accès aux données pour ces services et l'interrogation directe de la B.N.G. (HIT/NO HIT avec en cas de HIT de l'information complémentaire) ne correspond pas aux besoins et processus de travail de ces services de renseignement qui doivent pouvoir disposer de l'ensemble des informations disponibles pour réaliser dans la plus grande discrétion un travail d'investigation pour déterminer si une personne représente ou non des risques en matière de terrorisme ou de radicalisme. À l'issue de cette enquête de renseignement et dans le cadre du principe du need to share, les services de renseignement reviendront vers les services de police compétents avec de l'information "enrichie".

Bien entendu, les modalités de cette réciprocité doivent être examinées avec tous les partenaires concernés de sorte que la police puisse disposer de manière optimale des informations des services de renseignement dont elle a besoin pour accomplir ses missions.

Enfin, les missions de police administrative qui justifient le recours à une banque de données technique ont été étendues à la catégorie de personnes faisant l'objet d'une mesure de police. Cet ajout correspond au besoin opérationnel des services de police de pouvoir utiliser des caméras ANPR afin d'assurer efficacement le suivi d'une mesure de police prise par une autorité compétente, telle que par exemple l'interdiction de lieux ou de passage.

TOELICHTING

DAMES EN HEREN,

Dit voorstel heeft betrekking op het beheer van persoonsgegevens en van informatie door de politiediensten. Meer concreet is er de noodzaak van een optreden van de wetgever teneinde:

1) de richtlijn 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 overheden 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") om te zetten;

2) de tenuitvoerlegging, voor de open bepalingen, van Verordening 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").

Voormelde Europese regelgeving kreeg reeds een eerste wettelijke verankering ingevolge de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit. Ingevolge deze wet werd de Commissie voor de Bescherming van de Persoonlijke Levenssfeer in overeenstemming gebracht met de AVG. Ze wordt omgevormd tot de Gegevensbeschermingsautoriteit en wordt vier bevoegdheden toegewezen die kunnen worden samengevat als volgt: (1) informatie en advies, (2) begeleiding van de verwerkingsverantwoordelijken, (3) controle en (4) sanctie.

De wet van 3 december 2017 bepaalt eveneens dat de Gegevensbeschermingsautoriteit niet bevoegd is voor het toezicht op de politiediensten voor wat betreft de verwerking van persoonsgegevens die onder het toepassingsgebied van de AVG vallen. Het toezicht op deze verwerkingen wordt uitgeoefend door het Controleorgaan op de politionele informatie (hierna "het Controleorgaan").

De wet gegevensbescherming bevat een afzonderlijke titel 2 inzake 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

DEVELOPPEMENTS

MESDAMES, MESSIEURS,

Cette proposition porte sur la gestion des données à caractère personnel et des informations par les services de police. Plus concrètement, l'intervention du législateur est nécessaire afin de:

1) transposer la directive 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 "Directive");

2) mettre en œuvre, pour les clauses ouvertes, le Règlement 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").

La réglementation européenne précitée a déjà trouvé un premier ancrage légal dans la loi du 3 décembre 2017 portant création de l'Autorité de protection des données. Cette loi a mis en conformité la Commission pour la protection de la vie privée avec le RGPD. Cette commission est devenue l'Autorité de protection des données et s'est vu attribuer quatre compétences, qui peuvent se résumer comme suit: (1) information et conseil, (2) accompagnement des responsables de traitement, (3) contrôle et (4) sanction.

La loi du 3 décembre 2017 prévoit également que l'Autorité de protection des données n'est pas compétente pour exercer un contrôle sur les services de police en ce qui concerne les traitements de données à caractère personnel qui tombent dans le champ d'application du RGPD. Le contrôle de ce type de traitements sera effectué par l'Organe de contrôle de l'information policière (ci-après "l'Organe de contrôle").

La loi relative à la protection des données contient un titre 2 spécifiquement consacré 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

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. Dit omvat niet alleen de taken van gerechtelijke politie, doch ook de taken van bestuurlijke politie en ordehandhaving (zie *Parl. St.* Kamer, DOC 54 3126/001, 68). Het betreft dus meer bepaald de omzetting van de hiervoor vernoemde Richtlijn.

Titel 2 van de wet gegevensbescherming stelt het algemeen kader vast. Dit wetsvoorstel vertaalt dit concreet in de bestaande operationele en statutaire wetgeving inzake de geïntegreerde politie.

Wij herhalen dat de politie een informatieverwerkende organisatie is en dan ook bijzondere aandacht dient te hebben voor hoe ze met informatie zal omgaan. De "informatiegestuurde politiezorg" is één van de basisbegrippen van de "excellente politiezorg". Informatie vormt een leidraad in het nemen van beslissingen door overheden en politiediensten op terrein. Hierbij hoort dan ook de geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens die zijn opgenomen in bestanden of die bestemd zijn om hierin op te nemen (artikel 26, alinea 1, 2°, wet gegevensbescherming).

Politiediensten dienen evenwel bij het vervullen van hun opdrachten van bestuurlijke en/of gerechtelijke politie tegelijkertijd te waken over de naleving en bij te dragen tot de bescherming van de individuele rechten en vrijheden, evenals tot de democratische ontwikkeling van de maatschappij (zie artikel 1, tweede lid, wet op het politieambt). Meer concreet betreft dit het grondrecht van de bescherming van de persoonlijke levenssfeer. Ter zake kan verwezen worden naar artikel 22 van de Grondwet, artikel 8 van het Europees Verdrag voor de Rechten van de Mens en de Fundamentele Vrijheden (hierna "EVRM") en de artikelen 7 en 8 van het Handvest van de Grondrechten van de Europese Unie.

In navolging van de voorzieningen in de AVG dient er dus te worden voorzien in een hoge mate van zowel bescherming als beveiliging van de persoonsgegevens en de verwerking hiervan. In het bijzonder dienen verwerkingsverantwoordelijken en functionarissen van gegevensbescherming te worden aangeduid, categorieën van gegevens te worden omschreven en een wettelijk kader tot stand te worden gebracht, met name door voorafgaande adviezen in te winnen, door een register van deze verwerkingen aan de toezichthoudende autoriteit ter beschikking te stellen en door logbestanden van de verwerkingen bij te houden.

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. Ceci comprend non seulement les missions de police judiciaire, mais également les missions de police administrative et de maintien de l'ordre (voir *Doc. parl.* Chambre, DOC 54 3126/001, 68). Il s'agit donc plus spécifiquement de la transposition de la Directive susvisée.

Le titre 2 de la loi relative à la protection des données fixe le cadre général. La présente proposition de loi traduit ce cadre de façon concrète dans la législation opérationnelle et statutaire actuelle de la police intégrée.

Nous répétons que la police est une organisation qui traite des informations et doit donc accorder une attention particulière à la façon dont elle les traite. La "fonction de police guidée par l'information" étant l'une des notions de base de l'"excellence dans la fonction de police", l'information constitue un fil conducteur dans la prise de décisions par les autorités et les services de police sur le terrain. Ceci concerne donc les traitements intégralement ou partiellement automatisés de données à caractère personnel figurant ou destinées à figurer dans des fichiers (article 26, alinéa 1er, 2°, de la loi relative à la protection des données).

Lors de l'exercice de leurs missions de police administrative ou judiciaire, les services de police doivent concomitamment veiller au respect et contribuer à la protection des libertés et des droits individuels, ainsi qu'au développement démocratique de la société (voir article 1er, alinéa 2, de la loi sur la fonction de police). Il s'agit plus concrètement du droit fondamental de protection de la vie privée. En la matière, nous pouvons renvoyer à l'article 22 de la Constitution, à l'article 8 de la Convention européenne des droits de l'homme et des libertés fondamentales (ci-après "CEDH") et aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

Conformément aux dispositions du RGPD, un degré élevé à la fois de protection et de sécurisation des données à caractère personnel et de leur traitement doit être assuré. Il convient notamment de désigner des responsables du traitement et des délégués à la protection des données, de définir des catégories de données, de mettre sur pied un cadre légal, notamment en recueillant des avis préalables aux traitements, en mettant un registre de ces traitements à la disposition de l'autorité de contrôle et en procédant à une journalisation des opérations de traitement.

Het recht op vergeten is ook een belangrijk element inzake gegevensbescherming. Reeds in 2014 had de wetgever dit recht voor operationele politionele gegevensbanken verankerd door de wet van 18 maart 2014. Dit voorstel houdt geen wijziging in van de algemene regels betreffende het bewaren van gegevens in operationele politionele gegevensbanken. Het wijzigt dus ook niet de regels die specifiek zijn voor de Algemene Nationale Gegevensbank (hierna "A.N.G.").

De opstellers van dit voorstel wensen niettemin te reageren op punt 10, paragraaf 5, van advies nr. 9 van 12 december 2018 van het Controleorgaan, waarin het de verenigbaarheid van deze regels met artikel 30 van de bovengenoemde wet gegevensbescherming in twijfel trekt.

Het algemene beginsel vervat in artikel 30, § 1, is evenwel van toepassing en niet de uitzondering van het tweede lid: de wet op het politieambt (hierna "WPA") bepaalt de maximale bewaartermijn en bij het verstrijken van deze periode worden de operationele politiegegevens gewist.

De maximale bewaartermijn voor de gegevens van de A.N.G. wordt berekend op basis van de cumulatie van de artikelen 44/9 en 44/10.

Anderzijds rust op de wetgever geen enkele verplichting om na afloop van een eerste periode ervoor te zorgen dat "een analyse moet worden uitgevoerd op basis van verschillende noodzakelijkheids- en proportionaliteitscriteria om te bepalen of het nodig is dat de gegevens bewaard blijven, en in voorkomend geval, de nieuwe bewaartermijn". Dit onderzoek is een mogelijkheid aangeboden aan de wetgever inzake de bewaring van persoonsgegevens.

Rechtsoverweging 26 van Richtlijn gaat in dezelfde richting wanneer zij stelt dat "om ervoor te zorgen dat de gegevens niet langer worden bewaard dan noodzakelijk, de verwerkingsverantwoordelijke termijnen moeten vaststellen met het oog op het wissen of op periodieke controle".

Bovendien worden de criteria van proportionaliteit en noodzakelijkheid op het gebied van gegevensbewaring toegepast, in die zin dat de toegang tot de archieven van het A.N.G. alleen is voorbehouden aan bepaalde profielen waaronder enkele leden van de politiediensten, in zeer strikte hypotheses en limitatief opgesomd in artikel 44/10.

Een effectieve en efficiënte controle van alle door de politie verwerkte gegevens vormen ook een belangrijk

Le droit à l'oubli est aussi un élément important en matière de protection des données. Déjà en 2014, le législateur avait consacré ce droit pour les banques de données policières opérationnelles par la loi du 18 mars 2014. La présente proposition ne modifie pas les règles générales relatives à la conservation des données dans les banques de données policières opérationnelles. Elle ne modifie donc pas non plus les règles qui sont spécifiques à la Banque de données Nationale Générale (ci-après "B.N.G.").

Les rédacteurs de la présente proposition souhaitent néanmoins répondre au point 10, alinéa 5 de l'avis n° 9 du 12 décembre 2018 de l'Organe de contrôle où il s'interroge sur la compatibilité de ces règles de conservation avec l'article 30 de la loi relative à la protection des données.

C'est le principe général contenu à l'article 30, § 1er, qui est d'application et non pas l'exception prévue à l'alinéa 2: la loi sur la fonction de police (ci-après "LFP") détermine la durée maximale de conservation et à l'échéance de cette durée, les données policières opérationnelles sont effacées.

Le délai maximal de conservation des données de la B.N.G. est calculé sur la base du cumul des articles 44/9 et 44/10.

Il n'y a d'ailleurs aucune obligation du législateur de prévoir à l'issue d'un premier délai qu'"une analyse soit effectuée sur la base de différents critères de nécessité et de proportionnalité afin de déterminer si la conservation des données doit être maintenue et, le cas échéant, le nouveau délai de conservation". Cet examen constitue une possibilité qui est laissée au législateur concernant la conservation des données à caractère personnel.

Le considérant 26 de la Directive va dans le même sens lorsqu'il stipule qu'"afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, des délais devraient être fixés par le responsable du traitement en vue d'un effacement ou d'un examen périodique".

Par ailleurs, les critères de proportionnalité et de nécessité sont mis en œuvre en matière de conservation des données dans le sens où l'accès aux archives de la B.N.G. est réservé à certains profils parmi les seuls membres des services de police, dans des hypothèses très strictes et énumérées limitativement à l'article 44/10.

Un contrôle efficace et effectif de l'ensemble des données traitées par la police constitue également un

element op niveau van bescherming van persoonsgegevens. De Richtlijn maakt het mogelijk deze controle uit te voeren door middel van de gegevensbeschermingsautoriteit, *in casu* het Controleorgaan. Dit soortgelijke recht voor de bevoegde autoriteiten in titel 2 van de wet gegevensbescherming is verankerd in artikel 41 van deze wet. Anderzijds voert artikel 42 dit indirecte toegangsmechanisme rechtstreeks in deze wet uit voor politiediensten. Het systeem van indirecte toegang voor politiediensten heeft reeds een duidelijke rechtsgrondslag.

De Commissie voor de bescherming van de persoonlijke levenssfeer heeft in haar aanbeveling nr. 04/2017 van 24 mei 2017 aangegeven dat het mogelijk was de functie van functionaris voor gegevensbescherming te cumuleren met andere functies, waaronder die van veiligheidsconsulent. De opstellers van de huidige tekst hebben daarom gebruik gemaakt van deze mogelijkheid, die het voordeel biedt, eenzelfde functie aan te wijzen belast met adviesverlening, wat betreft het beheer van operationele en niet-operationele politionele gegevens evenals de aspecten verbonden aan het privéleven als deze betreffende de veiligheid.

Anderzijds neemt om die reden artikel 44/3, § 1, vijfde lid, de opdrachten vervat in artikel 65 van de wet gegevensbescherming over om ze ook van toepassing te maken op het veiligheidsaspect van de verwerking.

Wat betreft de overdracht van politiegegevens die aanvankelijk voortkwamen uit de verwerking door de politiediensten van gegevens in het kader van titel 2 (operationele verwerking) aan een politiedienst of een administratief orgaan handelend op grond van titel 1 (bv. interne controle (bv. de tuchtraad), wijst de Raad van State in zijn advies 65.312/2 van 4 maart 2019 erop dat artikel 14 van de wet gegevensbescherming volstaat en dat deze bepaling derhalve niet in de wet op de geïntegreerde politie hoeft te worden overgenomen. Om verwarring te voorkomen hebben de opstellers daarom dit voorgestelde artikel geschrapt.

Ten slotte geeft het Controleorgaan in zijn hoedanigheid van "*Data Protection Authority*" voor de politiediensten op verschillende plaatsen in zijn advies nr. 9 van 12 december 2018 (zie bijvoorbeeld de punten 18 en 19) aan dat zijn advies moet worden ingewonnen alvorens een wettelijke norm op te maken inzake verwerking van operationele of niet-operationele politionele informatie. Deze toevoegingen lijken echter niet noodzakelijk. Inderdaad, zoals de Richtlijn, de AVG evenals de wet gegevensbescherming de regels vastleggen over de bevoegdheid van de bevoegde autoriteit om adviezen

élément important au niveau de la protection des données à caractère personnel. La Directive permet que ce contrôle soit effectué par le truchement de l'autorité de protection des données, *in casu* l'Organe de contrôle. Ce droit générique pour les autorités compétentes du titre 2 de la loi relative à la protection des données est consacré à l'article 41 de cette loi. Par ailleurs, l'article 42 exécute directement dans cette loi ce mécanisme d'accès indirect pour les services de police. Le système d'accès indirect pour les services de police a donc déjà une assise légale claire.

Dans sa recommandation 04/2017 du 24 mai 2017, la Commission de la protection de la vie privée a indiqué qu'il était possible de cumuler la fonction de délégué à la protection des données avec d'autres fonctions dont celle de conseiller en sécurité. Les rédacteurs du présent texte ont donc fait usage de cette possibilité qui offre l'avantage, pour ce qui concerne la gestion des données policières opérationnelles et non opérationnelles, de désigner une même fonction chargée de donner des avis concernant tant des aspects liés à la protection des données que ceux relatifs à la sécurité des systèmes d'information.

C'est d'ailleurs pour cette raison que l'article 44/3, § 1er, alinéa 5, reprend les missions contenues dans l'article 65 de la loi relative à la protection des données pour les adjoindre aux autres missions portant sur la sécurité des traitements.

Pour ce qui concerne le transfert de données policières émanant initialement d'un traitement réalisé par les services de police dans le cadre du titre 2 (traitement opérationnel) vers un service de police ou un organe administratif agissant dans le cadre du titre1er (par exemple un service chargé du contrôle interne) ou un organe administratif (par exemple le conseil de discipline), le Conseil d'État, dans son avis 65.312/2 du 4 mars 2019, fait remarquer que l'article 14 de la loi relative à la protection des données est suffisant et qu'il n'y a donc pas lieu de recopier cette disposition dans la loi sur la police intégrée. Afin d'éviter toute confusion, les rédacteurs ont donc supprimé cet article proposé.

Enfin, l'Organe de contrôle, dans sa compétence de "*Data Protection Authority*" des services de police, indique à plusieurs endroits de son avis n° 9 du 12 décembre 2018 (voir par exemple les points 18 et 19) qu'il souhaite que son avis soit demandé préalablement à l'établissement d'une norme juridique en matière de traitement relatif à l'information policière opérationnelle ou non opérationnelle. Ces ajouts ne semblent cependant pas nécessaires. En effet, tant la Directive que le RGPD et la loi relative à la protection des données fixent les règles relatives à la compétence d'avis de l'autorité

te geven in het kader van de voorbereiding van een wet, decreet of ordonnantie, of een op een dergelijke wet, decreet of ordonnantie gebaseerde regelgevende maatregel, die betrekking heeft op de verwerking van persoonsgegevens. Het is derhalve niet nodig om er in elk artikel aan te herinneren dat een dergelijke norm met betrekking tot de verwerking van persoonsgegevens onderworpen is aan het advies van het Controleorgaan. *A contrario*, indien deze normen geen betrekking hebben op de verwerking van persoonsgegevens, is het natuurlijk niet nodig om de bevoegde toezichthoudende autoriteit voor gegevensbescherming te raadplegen.

Dit wetsvoorstel voorziet in de wettelijke verankering van deze voorzieningen.

ARTIKELSGEWIJZE BESPREKING

TITEL II

Wijzigingsbepalingen

HOOFDSTUK I

Wijzigingen van de wet op het politieambt

Artikel 2 (wijziging artikel 3)

Gelet op de ingrijpende wijzigingen in het informatielandschap, dit ingevolge de invoering van de AVG en de wet gegevensbescherming, en gelet op het feit dat het Controleorgaan aangeduid wordt als bevoegde toezichthoudende autoriteit voor alle informatieverwerking door politiediensten, was er noodzaak aan een actualisering van deze definitie.

In de wet gegevensbescherming wordt er uitdrukkelijk een rol toegewezen aan het Controleorgaan, met als sleutelartikel artikel 71. Door hiernaar te verwijzen bij de begripsomschrijving van het Controleorgaan, wordt duidelijk de link gemaakt tussen enerzijds de WPA, de basistekst voor de politiediensten en in het bijzonder de basis voor de politionele gegevensverwerking, en anderzijds de regelgeving betreffende bescherming van persoonsgegevens en in het bijzonder de bevoegdheden van het voor de politiediensten bevoegde toezichthouden autoriteit, te weten het Controleorgaan.

Aangezien het duidelijk is dat de wet gegevensbescherming een sleutelrol speelt en meermaals aangehaald wordt en zal worden in de WPA, leek het gepast om deze ook te definiëren. Alleen al omwille van de leesbaarheid van de wettekst, drong dit zich op.

de contrôle compétente dans le cadre de l'élaboration d'une loi, d'un décret ou d'une ordonnance, ou d'une mesure réglementaire fondée sur une telle loi, un tel décret ou une telle ordonnance, qui se rapporte au traitement de données à caractère personnel. Il n'est donc pas nécessaire de rappeler dans chaque article qu'une telle norme qui se rapporte au traitement de données à caractère personnel est soumise à l'avis de l'Organe de contrôle. *A contrario*, si ces normes ne portent pas sur le traitement de données à caractère personnel, il n'y a bien entendu pas lieu de consulter l'autorité de contrôle compétente en matière de protection des données.

La présente proposition de loi permet l'ancrage légal de ces dispositions.

COMMENTAIRE DES ARTICLES

TITRE II

Dispositions modificatives

CHAPITRE I^ER

Modifications de la loi sur la fonction de police

Article 2 (modification de l'article 3)

Etant donné les importantes modifications en matière d'information qu'a entraîné l'entrée en vigueur du RGPD et de la loi relative à la protection des données, et le fait que l'Organe de contrôle est désigné comme autorité de contrôle compétente pour l'ensemble des traitements d'informations par les services de police, il était nécessaire d'actualiser cette définition.

La loi relative à la protection des données confère un rôle explicite à l'Organe de contrôle, en particulier à l'article 71. La référence à cet article dans la définition de l'Organe de contrôle met clairement en exergue le lien entre d'une part la LFP, qui est le texte fondamental des services de police, en particulier en ce qui concerne le traitement de données par la police, et d'autre part la réglementation en matière de protection des données à caractère personnel, et en particulier les compétences de l'autorité de contrôle compétente pour les services de police, à savoir l'Organe de contrôle.

Dans la mesure où il est clair que la loi relative à la protection des données joue un rôle fondamental et est, et sera citée à plusieurs reprises dans la LFP, il paraissait judicieux de la définir également. Cela s'imposait, ne fût-ce que par souci de lisibilité du texte de loi.

Artikel 3 (wijziging artikel 25/8)

Aangezien de Gegevensbeschermingsautoriteit niet langer de bevoegde toezichthoudende autoriteit is voor de informatieverwerking door politiediensten, dient dit artikel te worden geactualiseerd. Het is immers overbodig om hen op de hoogte te brengen, aangezien zij niet langer bevoegd zijn voor wat betreft politionele gegevensverwerkingen.

Daarnaast dient de veiligheidsconsulent ook niet langer op de hoogte te worden gebracht, aangezien deze werd vervangen door de functie van functionaris voor gegevensbescherming.

Het register dat alle cameragebruiken bevat zoals bepaald in artikel 25/8, eerste lid, wordt opgenomen in het register dat bij de politiediensten is ingesteld door het nieuwe artikel 145 van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus. (zie *infra* artikel 32).

Dit artikel betreft dus voornamelijk een technische aanpassing.

Article 3 (modification de l'article 25/8)

L'Autorité de protection des données n'étant plus l'autorité de contrôle compétente pour les traitements d'informations par les services de police, cet article doit être actualisé. Il s'avère en effet superflu d'informer cette Autorité dès lors qu'elle n'est plus compétente à l'égard des traitements de données policières.

De même, le conseiller en sécurité ne doit plus être informé, dans la mesure où il a été remplacé par la fonction de délégué à la protection des données.

Le registre reprenant toutes les utilisations de caméras visé à l'alinéa premier de l'article 25/8 est intégré dans le registre mis en place au sein des services de police par le nouvel article 145 de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (voir *infra* article 32).

Cet article consiste donc essentiellement en une adaptation technique.

Artikel 4 (wijziging artikel 44/1)

Opdat een verwerking van persoonsgegevens door politiediensten rechtmatig zou zijn, dienen er bepaalde verplichtingen te worden voldaan, zoals omschreven in artikel 33 van de wet gegevensbescherming.

Er werd hierboven reeds aangehaald dat de categorieën van persoonsgegevens moeten verduidelijkt worden in een wettelijke bepaling (die gebeurt in het aangepaste artikel 44/5 WPA, zie *infra*). Daarnaast dienen ook de doeleinden van de verwerking verduidelijkt te worden, hetgeen de aanleiding is voor de aanpassing van artikel 44/1.

De opdrachten van de politiediensten, bedoeld in hoofdstuk III, afdeling 1, (waarnaar nu al verwezen wordt in artikel 44/1 WPA) verwoorden reeds de opdrachten en de doeleinden van informatieverwerking door de politiediensten.

Bijgevolg was WPA hiermee reeds in regel. Door echter ook artikel 27 van de wet gegevensbescherming uitdrukkelijk aan te halen, wordt bijkomend verduidelijkt dat alle politionele opdrachten, zowel bestuurlijke als gerechtelijke, vallen onder de omschrijving gegeven in voormeld artikel. Hiervoor kan tevens verwezen worden naar de memorie van toelichting bij de wet gegevensbescherming, waarin duidelijk uiteengezet wordt dat

Article 4 (modification de l'article 44/1)

Pour qu'un traitement de données à caractère personnel par les services de police soit licite, certaines obligations doivent être remplies, comme prévu à l'article 33 de la loi relative à la protection des données.

Il a déjà été indiqué ci-dessus que les catégories de données à caractère personnel doivent être précisées par le biais d'une disposition légale (qui passe par une adaptation de l'article 44/5 de la LFP, voir *infra*). Les finalités du traitement doivent également être précisées, ce qui entraîne l'adaptation de l'article 44/1.

Les missions des services de police, visées au chapitre III, section 1re, (à laquelle il est d'ores et déjà fait référence à l'article 44/1 de la LFP), définissent déjà les missions et les finalités des traitements d'informations par les services de police.

La LFP était donc déjà conforme à ces dispositions. Toutefois, la référence explicite à l'article 27 de la loi relative à la protection des données met en évidence le fait que toutes les missions de police, qu'elles soient administratives ou judiciaires, sont couvertes par la définition donnée à l'article précité. En la matière, il convient également de renvoyer à l'exposé des motifs de la loi relative à la protection des données, qui précise

alle opdrachten van gerechtelijke en bestuurlijke politie vallen onder het toepassingsgebied van titel 2 van de wet gegevensbescherming:

"Voor de duidelijkheid wordt ook bevestigd dat dit, naast de taken van de gerechtelijke politie, ook de taken van bestuurlijke politie omvat. Klassiek kan verwezen worden naar de handhaving van de openbare orde. De openbare orde omvat de klassieke trilogie bestaande uit openbare rust, veiligheid en gezondheid. De openbare rust beoogt de afwezigheid van wanordelijkheden en onlusten in openbare plaatsen. De openbare veiligheid beoogt de afwezigheid van gevaarlijke toestanden voor personen en goederen en omvat o.m. de voorkoming van de criminaliteit en de bijstand van de personen in gevaar. De openbare gezondheid beoogt de afwezigheid van ziekten door de handhaving van de hygiëne en door het vrijwaren van een kwalitatief leefmilieu. Dit begrip openbare orde wordt aldus bepaald als leidraad van en maatstaf voor het optreden van de politiediensten en legt de nadruk op de noodzaak van het daadwerkelijk behoud van de openbare orde." (*Parl. St.* Kamer, DOC 54 3126/001, 68)

De verwijzing naar het artikel 34 van de wet gegevensbescherming betreft in eerste instantie een eerder technische aanpassing, aangezien hetgeen vroeger geregeld werd in artikel 6 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (hierna "Privacywet"), nu geregeld wordt in artikel 34 van de wet gegevensbescherming.

De verplichting om een KB op te stellen wordt daarnaast ook opgeheven, enerzijds gelet op het feit dat er door de wet gegevensbescherming reeds voorzien wordt in algemene regels die destijds bij KB dienden te worden vastgelegd en anderzijds gelet op het feit dat het wetsvoorstel expliciete regels en/of beperkingen oplegt voor bijzondere categorieën van gegevens bedoeld in het artikel 34 van de wet gegevensbescherming.

Tevens werd, om redactionele redenen, ervoor gekozen om "verzamelen" ter verwijderen, aangezien het inbegrepen is in de term "verwerken". Het betreft hier een onnodige verwarring.

De persoonsgegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, het lidmaatschap van een vakvereniging blijken evenals de gegevens betreffende het seksueel gedrag of seksuele gerichtheid van een natuurlijke persoon worden enkel en alleen incidenteel verwerkt betreffende een hoofdverwerking

que toutes les missions de police judiciaire et administrative font partie du champ d'application du titre 2 de la loi relative à la protection des données:

"Dans un souci de clarté, il est également confirmé que, outre les tâches de police judiciaire, cela inclut également les tâches de police administrative. Il peut traditionnellement être renvoyé au maintien de l'ordre public. L'ordre public consiste en la trilogie classique, comprenant la tranquillité, la sécurité et la santé publiques. La tranquillité publique vise l'absence de troubles et d'émeutes dans les endroits publics. La sécurité publique vise l'absence de situations dangereuses pour les personnes et les biens, et comprend entre autres la prévention de la criminalité et l'assistance aux personnes en danger. La santé publique vise l'absence de maladies en maintenant l'hygiène et en préservant un cadre de vie qualitatif. Cette notion d'ordre public est donc définie comme fil conducteur et norme pour les interventions des services de police et met l'accent sur la nécessité de maintenir effectivement l'ordre public." (*Doc. parl.* Chambre, DOC 54 3126/001, 68)

La référence à l'article 34 de la loi relative à la protection des données consiste tout d'abord en une adaptation plutôt technique, dans la mesure où ce qui était précédemment déjà régi par l'article 6 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 (ci-après "loi vie privée") se trouve à présent régi par l'article 34 de la loi relative à la protection des données.

L'obligation de rédiger un AR est également supprimée, d'une part en raison du fait que la loi relative à la protection des données contient déjà des règles générales qui devaient anciennement être fixées par AR, et d'autre part en raison du fait que la proposition de loi impose des règles et/ou restrictions explicites pour des catégories particulières de données visées à l'article 34 de la loi relative à la protection des données.

Pour des raisons rédactionnelles, le choix a également été fait de supprimer le mot "collecter" dans la mesure où cette notion est englobée dans le terme "traiter". Il s'agit d'une source inutile de confusion.

Les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ainsi que les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont uniquement traitées de manière incidente par rapport à un traitement principal portant sur l'une

die betrekking heeft op één van de in artikel 44/5 voornoemde categorieën van gegevens. Dit zal bijvoorbeeld het geval zijn voor een onderzoek betreffende homofobe agressies.

Ingevolge de punten 4 en 5 van advies nr. 9 van het Controleorgaan van 12 december 2018, wordt artikel 44/1, § 2, aangepast door enerzijds het begrip "verwerking die niet tot hoofddoel strekt" van de in artikel 34 van de wet gegevensbescherming bedoelde gegevens te schrappen en anderzijds door het begrip "gevoelige gegevens die niet zijn gedefinieerd" te schrappen. Wat dit laatste aspect betreft, hebben de opstellers van dit voorstel besloten rechtstreeks te verwijzen naar de bijzondere categorieën van gegevens bedoeld in artikel 34 van de wet gegevensbescherming. Het is derhalve niet langer nodig dit begrip van gevoelige gegevens te definiëren, aangezien het niet langer wordt gebruikt.

Betreffende de biometrische gegevens voorziet deze bepaling in de verwerking van biometrische gegevens door de politie naast andere categorieën van gegevens bepaald in artikel 44/5, inzake bestuurlijke, gerechtelijke politie alsook inzake internationale politionele samenwerking.

De verwerking van deze gegevens heeft uitsluitend de zekere identificatie van personen tot doel. Dit doel kan niet bereikt worden met andere middelen, zoals de controle van identiteits- of reisdocumenten of de raadpleging van gegevensbanken op alfanumerieke basis. In dergelijke gevallen is het risico op identiteitsfraude of fouten groot.

De betrokken biometrische gegevens zijn onder andere afkomstig van de inschrijving van personen in verdenking gesteld, de sporenopname op de plaats delict of de internationale uitwisseling van gegevens. Op dit ogenblik hebben deze betrekking op vingerafdrukken, gezichtskenmerken, stem, oorafdruk en zouden zich kunnen uitbreiden tot gegevens zoals de iris of de voortbeweging.

De richtlijnen betreffende de verwerking van biometrische gegevens gaan uit van de bevoegde ministers, de korpschefs, de commissaris-generaal, de directeurs-generaal of de directeurs en worden in ieder geval voorafgegaan door een beoordeling van het effect zoals bepaald in artikel 58 van de wet gegevensbescherming.

Er wordt uitdrukkelijk melding gemaakt van dit artikel 58 van de wet gegevensbescherming, die in bepaalde gevallen voorziet in een gegevensbeschermingseffectenbeoordeling.

des catégories de données énumérées à l'art. 44/5. Tel sera par exemple le cas d'une enquête portant sur des agressions homophobes.

Suite aux points 4 et 5 de l'avis n° 9 du 12 décembre 2018 de l'Organe de contrôle, l'article 44/1, § 2, est adapté, d'une part, en supprimant la notion de "traitement n'ayant pas pour objet principal" les données visées à l'article 34 de la loi relative à la protection des données et, d'autre part, en supprimant la notion de données sensibles qui n'était pas définie. Pour ce dernier aspect, les rédacteurs de la présente proposition ont décidé de faire directement référence aux catégories particulières de données visées à l'article 34 de la loi relative à la protection des données. Il n'y a donc plus lieu de définir cette notion de données sensibles puisqu'elle n'est plus utilisée.

En ce qui concerne ensuite les données biométriques, cette disposition prévoit le traitement de données biométriques par la police en complément d'autres catégories de données prévues à l'article 44/5, en matière de police administrative, judiciaire ainsi qu'en matière de coopération policière internationale.

Le traitement de ces données a pour seul but l'identification certaine de personnes. Cet objectif ne peut pas être atteint par d'autres moyens, comme par exemple le contrôle de documents d'identité ou de voyage ou la consultation de banques de données sur base alphanumérique. En pareils cas, les risques de fraude à l'identité ou d'erreur sont importants.

Les données biométriques concernées proviennent entre autres de l'enregistrement des personnes suspectées, du relevé de traces sur les scènes de crime, voire de l'échange international de données. Elles concernent actuellement les empreintes digitales, les traits du visage, la voix, l'empreinte des oreilles et pourraient s'étendre à d'autres données telles que l'iris ou la démarche.

Les directives concernant le traitement de données biométriques sont prises par les ministres compétents, les chefs de corps, le Commissaire général, les directeurs généraux ou les directeurs et sont en tout état de cause précédées par une analyse d'impact telle que prévue à l'article 58 de la loi relative à la protection des données.

Il est explicitement fait mention de cet article 58 de la loi relative à la protection des données, qui prévoit dans certains cas une analyse d'impact relative à la protection des données.

Deze regels dienen dan wel steeds nageleefd te worden, maar het werd opportuun geacht om dit nog eens uitdrukkelijk te vermelden.

De bestaande gegevensbanken die reeds zijn opgericht en aangegeven bij het Controleorgaan zijn in beginsel slechts onderhevig aan het uitvoeren van een gegevensbeschermingseffectbeoordeling indien de risico's voor de rechten en vrijheden voor natuurlijke personen veranderen, bijvoorbeeld omdat een nieuwe technologie in gebruik is genomen (vgl. randnummers 101-104 aanbeveling nr. 1/2018 Gegevensbeschermingsautoriteit).

De bepaling aangaande de gezondheidsgegevens wordt ingevoegd omwille van het feit dat politieambtenaren en beveiligingsassistenten en -agenten van politie, maar ook de personen die aan hun bescherming zijn toevertrouwd, hulpverleningspersoneel, arrestanten, advocaten die bijstand geven (meer bepaald voor vertrouwelijk overleg) in het kader van verhoren, gerechtsdeskundigen (tolken) steeds het risico lopen om besmet te worden met een zwaar besmettelijke ziekte. Dit risico loopt men bij vechtpartijen, fouilleringen, bijtincidenten, arrestaties, …

Naast het emotioneel beheer blijft men nog met andere vragen zitten, zoals de grote onzekerheid omtrent het feit van een eventuele besmetting. Medische testen naar bepaalde besmettelijke ziekten kunnen vaak pas maanden na de vermoedelijke besmetting uitsluitsel geven. Ondertussen blijft de betrokkene, maar ook zijn familie met de pijnlijke onzekerheid zitten. Eenzelfde situatie kan ook aanleiding geven tot arbeidsongeschiktheid.

In sommige gevallen is er ook een belang om een snelle interventie toe te laten met het oog op het nemen van postexpositie profylaxe medicatie. Zo kan bij voorbeeld na een prikincident een behandeling met HIV-remmers (liefst binnen 2 uur, maximaal 72 uur) nodig zijn om het risico van infectie zo klein mogelijk te maken. De behandeling met HIV-remmers geeft soms bijwerkingen Daarom is het belangrijk om een goede afweging te maken tussen het gelopen risico en de last van de behandeling.

Daarenboven is het op basis van informatie bij vorige confrontaties nuttig om te weten waarom er zich bij een betrokkene een plotse stemmingswisseling of paniekreactie kan voordoen. Bij bepaalde personen met een ontwikkelingsstoornis kan een bepaalde situatie immers een hevige reactie uitlokken. Het is van

Même si ces règles doivent dans tous les cas être respectées, il a paru opportun de les mentionner expressément une nouvelle fois.

Les bases de données existantes qui ont déjà été créées et déclarées à l'Organe de contrôle ne sont en principe soumises à une analyse d'impact sur la protection des données que si les risques pour les droits et libertés des personnes physiques évoluent, par exemple parce qu'une nouvelle technologie est utilisée (*cf.* les points 101-104 de la recommandation n° 1/2018 de l'autorité de protection des données).

La disposition concernant les données relatives à la santé est insérée en raison du fait que les fonctionnaires de police et les assistants et agents de sécurisation de police, ainsi que les personnes placées sous leur protection, le personnel de secours, les personnes arrêtées, les avocats qui prêtent leur assistance dans le cadre d'auditions (notamment pour la concertation confidentielle) et les experts judiciaires (interprètes) courent toujours le risque d'être contaminés par des maladies hautement contagieuses. Ce risque se pose en cas de bagarres, fouilles, incidents impliquant des morsures, arrestations, …

Au-delà de la gestion émotionnelle, d'autres questions subsistent, comme la grande incertitude quant à une éventuelle contamination. Les tests médicaux concernant certaines maladies infectieuses ne peuvent souvent livrer un résultat certain que des mois après l'infection présumée. En attendant, la personne concernée, tout comme sa famille, reste confrontée à une douloureuse incertitude. Pareille situation peut également engendrer une incapacité de travail.

Dans certains cas, il y a également un intérêt à permettre une intervention rapide en vue d'un traitement médicamenteux prophylactique post-exposition. Par exemple, après un incident impliquant un contact avec une seringue, un traitement à l'aide d'inhibiteurs du VIH peut être nécessaire (de préférence dans les 2 heures, et au maximum dans les 72 heures) afin de réduire au maximum le risque d'infection. Comme le traitement à l'aide d'inhibiteurs du VIH provoque parfois des effets secondaires, il est nécessaire d'effectuer une juste appréciation entre le risque encouru et la charge du traitement.

De surcroît, il peut être utile de savoir, en fonction d'informations obtenues lors de précédentes confrontations, pourquoi un changement d'humeur soudain ou une réaction de panique peut se produire chez une personne concernée. Chez certaines personnes présentant un trouble du développement, certaines situations

belang dat wanneer dit bij een vorige interventie aan het licht is gekomen, dit element kan verwerkt worden. Informatie in die zin kan ook nuttig zijn met het oog op de opsluiting van een persoon. Dit kan de politie doen besluiten om te voorzien in aangepaste maatregelen bij opsluiting (aanvullend toezicht, ...) in het belang van de gezondheid van de persoon die het voorwerp uitmaakt van een bestuurlijke of gerechtelijke vrijheidsbeneming.

De politiediensten kunnen om die reden op basis van verkregen informatie (bv. betrokkene heeft het spontaan gemeld) of ervaringen bij vorige interventies (bv. plotse stemmingswisseling of paniekreactie bij een opsluiting, agressie tegen medearrestanten, ...) bepaalde informatie hebben. Bij verwerking van een categorie van persoonsgegevens zoals bepaald in artikel 44/5 WPA kan een bepaalde te nemen maatregel toegevoegd worden. Het kan evenwel geen aanleiding geven tot discriminerende maatregelen en overdreven beveiligingsmaatregelen (bv. al te opzichtige beschermingskledij). De bedoeling is enkel de onvoorziene interventies, of te voorziene interventies (inschatting van risico's bij een overbrenging van een persoon naar de gevangenis of voorleiding voor een magistraat) op een veilige wijze te laten verlopen. Inzonderheid kan alvorens op te treden het personeel op de hoogte worden gebracht (bv. interventieploeg op weg naar een opdracht, de voorgenomen arrestatie van een gekend persoon, de bijstand te leveren aan een gerechtsdeurwaarder, ...).

Er kan verwezen worden naar artikel 2 EVRM en de positieve verplichting van een staat om de burgers te beschermen wanneer er een reële dreiging tegen hun leven (en gezondheid) bestaat. Daarnaast is het ook zo dat de wetgever reeds voorzien heeft in een mogelijkheid om een verdachte te verplichten mee te werken aan een bloedtest om na te gaan dat bij het plegen van een misdrijf geen besmettelijke ziekte werd overgedragen. (artikelen 524*quater* e.v. wetboek van strafvordering).

Om te antwoorden op de vraag van het Controleorgaan op de verwerking van gegevens betrekkelijk de gezondheid (punt 6 van het advies nr.9 van 12 december 2018), moet goed begrepen worden dat de omstandigheid verbonden aan de betrokken persoon van toepassing is op het geheel van bestuurlijke en gerechtelijke politionele opdrachten en de verwijzing naar de "betrokken persoon" strekt tot alle categorieën van personen bedoeld in het artikel 44/5. De bovengenoemde voorbeelden zijn geenszins exhaustief.

Ten slotte beperkt de politie zich, betreffende de genetische gegevens, tot het verzamelen van genetische

peuvent en effet provoquer des réactions violentes. Lorsque de telles réactions sont apparues lors d'une précédente intervention, il est important que cet élément d'information puisse être traité. Les informations en ce sens peuvent également s'avérer utiles par rapport à l'enfermement d'une personne. Elles peuvent conduire la police à décider de prévoir des mesures adaptées en cas d'enfermement (surveillance complémentaire, ...) dans l'intérêt de la santé de la personne qui fait l'objet d'une privation de liberté administrative ou judiciaire.

Les services de police peuvent dès lors disposer de certaines informations sur la base d'éléments directement obtenus (p.e.: la personne concernée l'a spontanément signalé), ou d'expériences vécues lors de précédentes interventions (p.e. changement d'humeur soudain ou réaction de panique lors de l'enfermement, agression envers d'autres personnes arrêtées, …). Le traitement d'une catégorie de données à caractère personnel tel que prévu à l'article 44/5 LFP peut être assorti de mesures à prendre. Cela ne peut toutefois entraîner de mesures discriminatoires ni de mesures excessives de sécurisation (p.e. une tenue de protection trop voyante). Le but est uniquement de permettre aux interventions, planifiées ou non (estimation des risques lorsqu'une personne est transférée en prison ou menée devant un magistrat), de se dérouler en toute sécurité. En particulier, le personnel peut être informé préalablement à l'intervention (p.e.: lorsqu'une équipe d'intervention part effectuer une mission, lors de l'arrestation d'une personne connue, lorsqu'une assistance est fournie à un huissier de justice, …).

Il peut être renvoyé à l'article 2 de la CEDH et à l'obligation positive d'un État de protéger les citoyens lorsqu'il existe une menace réelle contre leur vie (et leur santé). En outre, le législateur prévoit également une possibilité d'obliger un suspect à coopérer à un test sanguin afin de vérifier si une maladie contagieuse a été transmise lors de la commission d'un délit. (articles 524*quater* e.s. Code d'instruction criminelle)

Pour répondre à la demande de précision de l'Organe de contrôle sur le traitements des données relatives à la santé point 6 de l'avis n° 9 du 12 décembre 2018), il faut bien comprendre que le contexte lié à la personne concernée s'applique à l'ensemble des missions de police administrative et de police judiciaire et la référence à la "personne concernée" vise toutes les catégories de personnes visées à l'article 44/5. Les exemples fournis *supra* sont aucunement exhaustifs.

Pour finir, concernant les données génétiques, la police se limite à rassembler les traces génétiques

sporen (DNA) en referentiemateriaal van personen (wet van 7 november 2011 betreffende identificatieprocedure via DNA onderzoek in strafzaken) met de noodzakelijke administratieve gegevens voor de *chain of custody*. De politie ontvangt informatie over de geanalyseerde sporen wat de bruikbaarheid daarvan en de mogelijke verbanden betreft (zie Col 21/2017).

Zoals overweging 37 van de Richtlijn in herinnering brengt, moeten voor alle in het kader van dit artikel 4 verwerkte gegevens geschikte waarborgen worden gegeven. Een van de geschikte waarborgen bestaat er natuurlijk in die gegevens slechts te verwerken als aanvulling op andere in het kader van de operationele opdrachten verwerkte gegevens.

Vervolgens werden de waarborgen voor de verwerking van de gevoelige gegevens vermeld in het koninklijk besluit van 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens integraal opgenomen in artikel 44/1, § 2*bis*, vijfde lid, met name dat:

— de lijst van categorieën van personen, die toegang hebben tot de persoonsgegevens, worden aangewezen door de verwerkingsverantwoordelijke of, in voorkomend geval, door de verwerker, met een beschrijving van hun functie ten aanzien van de verwerking van de gegevens in kwestie;

— de lijst van de categorieën van de aangewezen personen om de in deze paragraaf bedoelde gegevens te verwerken, door de verwerkingsverantwoordelijke of, in voorkomend geval, door de verwerker ter beschikking wordt gesteld van het Controleorgaan;

— de aangewezen personen, op grond van een wettelijke of statutaire verplichting, of een overeenkomstige contractuele bepaling, het vertrouwelijke karakter van de gegevens in kwestie in acht moeten nemen.

Drie bijkomende waarborgen inzake bescherming van de betrokken personen werden toegevoegd.

Het gaat er in de eerste plaats om, een onderscheid te maken tussen de in artikel 44/5 bedoelde categorieën van personen. Op die manier zullen de systemen voor de gegevensverwerking bijvoorbeeld duidelijk aangeven of de verwerkte gegevens over de politieke opvattingen een verdachte of een slachtoffer betreffen dat precies wegens die opvattingen zou worden vervolgd.

Vervolgens moeten technische en organisatorische maatregelen getroffen worden tegen toevallige of

(ADN) et le matériel de référence de personnes (loi du 7 novembre 2011 relative à la procédure d'identification au travers de recherche ADN dans des dossiers pénaux) avec les données administratives nécessaires pour la "*chain of custody*". La police reçoit des informations sur les traces analysées quant à leur caractère exploitable et les liens potentiels (voir Col 21/2017).

Comme le rappelle le considérant 37 de la Directive, il convient d'apporter des garanties appropriées pour l'ensemble des données traitées dans le cadre de cet article 4. Une des garanties appropriées consiste bien entendu à ne traiter ces données qu'en complément d'autres données traitées dans le cadre des missions opérationnelles.

Ensuite, les garanties entourant le traitement des données dites sensibles qui étaient mentionnées dans l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements ont été intégralement reprises dans le 44/1, § 2*bis*, alinéa 5, à savoir le fait que:

— la liste des catégories de personnes, ayant accès aux données à caractère personnel, sont désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description de leur fonction par rapport au traitement des données visées;

— la liste des catégories des personnes ainsi désignées pour traiter les données visées dans ce paragraphe est tenue à la disposition de l'Organe de contrôle par le responsable du traitement ou, le cas échéant, par le sous-traitant;

— les personnes désignées sont tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.

Trois garanties supplémentaires en matière de protection des droits des personnes concernées ont été ajoutées.

Il s'agit tout d'abord, de faire une distinction entre les catégories de personnes visées à l'article 44/5. De la sorte, les systèmes de traitement des données devront par exemple clairement indiquer si les données relatives aux opinions politiques qui sont traitées concernent un suspect ou une victime qui serait persécutée précisément en raison de celles-ci.

Ensuite, de mesures techniques et organisationnelles doivent être prises contre la destruction accidentelle

niet-toegelaten vernietiging, tegen toevallig verlies of tegen de wijziging of elke andere niet-toegelaten verwerking van die gegevens. Die maatregelen zijn zeer ruim en betreffen in het bijzonder de veiligheid van de fysieke toegangen tot de lokalen waar die gegevens worden verwerkt en de toegangen tot de gegevens. Bij wijze van voorbeeld, de politielaboratoria waar biometrische gegevens worden verwerkt, maken het voorwerp uit van veiligheidsregels wat de fysieke toegangen alsook de toegangen tot de verwerkte gegevens betreft.

Tot slot wordt aan de verwerkingsverantwoordelijken gevraagd in hun gegevensbeschermingsbeleid de concrete maatregelen op te nemen die ze zullen nemen om de opvolging van die categorieën van gegevens te verzekeren.

De bevoegde functionarissen voor gegevensbescherming zullen de opvolging van de toepassing van dat beleid, waaronder de naleving van de maatregelen voor de verwerking van de gevoelige gegevens, op zich nemen. Daartoe zullen ze bijvoorbeeld gerichte controles op die maatregelen of algemene controles op alle punten van het veiligheidsbeleid doorvoeren.

De Koning krijgt een volmacht om andere geschikte maatregelen te kunnen treffen. Betreffende het advies van de Raad van State 65.312/2 van 4 maart 2019 wordt gepreciseerd dat de waarborgen die de Koning kan bieden, aanvullend zijn op deze die reeds in dit artikel zijn voorzien. Het kan natuurlijk niet de bedoeling zijn dat de Koning de waarborgen die in dit artikel worden gesteld met betrekking tot de verwerking van bijzondere categorieën van persoonsgegevens beperkt, maar veeleer versterkt door ze aan te vullen indien nodig.

Artikel 5 (wijziging opschrift)

Aangezien de functie van veiligheidsconsulent vervangen wordt door die van functionaris voor gegevensbescherming (DPO) en gelet op het feit dat de bepalingen met betrekking hierop verplaatst worden naar de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus (hierna “WGP”) (zie *infra* artikel 31), kent dit opschrift geen nut meer.

Artikel 6 (wijziging artikel 44/3)

Zoals hierboven reeds gezegd, komt de functie van DPO in de plaats van de veiligheidsconsulent en worden de op deze functie toepasselijke regels overgeheveld naar de WGP.

ou non autorisée, contre la perte accidentelle ainsi que contre la modification ou tout autre traitement non autorisé de ces données. Ces mesures sont très larges et couvrent notamment la sécurité des accès physiques aux locaux où ces données sont traitées et les accès aux données. À titre illustratif, les laboratoires de la police où des données biométriques sont traitées font l’objet de règles de sécurité d’accès physiques ainsi qu’aux données traitées.

Enfin, il est demandé aux responsables du traitement d’indiquer dans leur politique de protection des données les mesures concrètes qu’ils vont prendre pour assurer le suivi de ces catégories de données.

Les délégués à la protection des données compétent assureront le suivi de la mise en œuvre de cette politique dont le respect des mesures prévues pour le traitement des données sensibles. Ils réalisent pour cela, par exemple, des contrôles ciblés sur ces mesures ou généraux sur l’ensemble des points de la politique de sécurité.

Une délégation est réalisée vers le Roi qui pourra prendre d’autres mesures appropriées. Concernant l’avis du Conseil d’État 65.312/2 du 4 mars 2019 sur ce point, il est précisé dans la loi que les garanties que le Roi peut apporter sont complémentaires à celles qui sont déjà prévues dans cet article. Il ne saurait bien entendu pas être question pour le Roi de revoir à la baisse les garanties énoncées par cet article en matière de traitement de catégories particulières de données à caractère personnel mais bien de les renforcer en les complétant si besoin.

Article 5 (modification de l’intitulé)

Dans la mesure où la fonction de conseiller en sécurité est remplacée par celle de délégué à la protection des données (DPO), et dès lors que les dispositions en la matière sont transférées dans la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (ci-après “LPI”) (voir *infra* article 31), cet intitulé n’a plus d’utilité.

Article 6 (modification article 44/3)

Comme mentionné ci-dessus, la fonction de délégué à la protection des données remplace celle de conseiller en sécurité et les règles régissant cette fonction sont transférées dans la LPI.

De reden voor deze overheveling is het feit dat de DPO niet enkel bevoegd zal zijn voor de politionele gegevensverwerking (geregeld in de WPA), maar ook voor de verwerking door politiediensten van gegevens die onder de AVG vallen.

De aanpassingen in artikel 44/3 WPA dienen aldus gelezen te worden in deze zin.

Echter, het toezicht over de gemeenschappelijk gegevensbanken (dat nu eenmaal geen AVG-karakter heeft) blijft wel in de WPA, gelet op de specificiteit ervan. De regelgeving hieromtrent wordt evenwel verplaatst naar de onderafdeling aangaande de gemeenschappelijke gegevensbanken, aangezien dit een correctere plaats is om dit te regelen (zie artikelen 44/11/3*quinquies*/1 e.v.).

De bepalingen betreffende de aanwijzing van de bevoegde DPO voor de gemeenschappelijke gegevensbanken worden eveneens verplaatst naar dezelfde onderafdeling.

Ten slotte wordt het artikel geactualiseerd verwijzend naar de nieuwe toepasselijke regelgeving en gebruik makend van de nieuwe en correcte terminologie.

Artikel 7 (wijziging artikel 44/4)

Naar aanleidingen van het in overeenstemming brengen van de politionele gegevensverwerking met de Europese regelgeving, maken we gebruik van de in de wet gegevensbescherming geregelde mogelijkheid om uitdrukkelijk de verwerkingsverantwoordelijke aan te duiden, dit teneinde elke mogelijke verwarring en discussie hieromtrent te vermijden.

Er wordt nu juridisch een feitelijkheid bevestigd: de ministers van Binnenlandse Zaken en Justitie zijn de verwerkingsverantwoordelijken voor de A.N.G. en de basisgegevensbanken, terwijl voor bijzondere gegevensbanken gekeken dient te worden naar de korpschefs, de commissaris-generaal, de directeurs-generaal of de directeurs die beslist hebben om verzamelde gegevens te verwerken in een bijzondere gegevensbank en hiervoor de doeleinden en middelen bepaald hebben.

Dit artikel bepaalt duidelijk wie de verantwoordelijken voor de verwerking zijn van de A.N.G. en de bijzondere gegevensbanken, te weten de minister van Binnenlandse Zaken voor wat betreft de gegevens verwerkt in het kader van de administratieve politie, en de minister van Justitie voor de gegevens verwerkt in het kader van de gerechtelijke politie, of allebei gezamenlijk wanneer het gaat om gegevens verwerkt in het kader van die twee finaliteiten.

Ce transfert s'explique par le fait que le DPO ne sera pas uniquement compétent pour les traitements de données policières (régis par la LFP) mais également pour les traitements effectués par les services de police de données tombant sous le champ d'application du RGPD.

Les modifications de l'article 44/3 de la LFP doivent être lues dans ce sens.

Toutefois, le contrôle des banques de données communes (qui n'est pas concerné par le RGPD) demeure bien dans la LFP, étant donné sa spécificité. La réglementation y afférente est toutefois transférée à la sous-section relative aux banques de données communes, dans la mesure où celle-ci est plus adéquate pour régir cette matière (voir articles 44/11/3*quinquies*/1 s.).

Les dispositions relatives à la désignation du DPO compétent pour les banques de données communes sont également déplacées vers la même sous-section.

Enfin, l'article est actualisé en faisant référence à la nouvelle réglementation applicable et en utilisant la nouvelle terminologie correcte.

Article 7 (modification article 44/4)

Dans le cadre de la mise en conformité des traitements de données policières avec la réglementation européenne, nous saisissons la possibilité offerte par la loi relative à la protection des données de désigner expressément les responsables du traitement, afin d'éviter toute confusion et toute discussion en la matière.

Une situation de fait se trouve désormais juridiquement confirmée: les ministres de l'Intérieur et de la Justice sont les responsables du traitement pour la B.N.G. et les banques de données de base, tandis que pour les banques de données particulières, il s'agit des chefs de corps, du commissaire général, des directeurs généraux ou des directeurs qui ont décidé de traiter des données collectées dans une banque de données particulière et ont déterminé les finalités et les moyens à cet effet.

Cet article indique clairement quels sont les responsables du traitement pour la B.N.G. et les banques de données particulières, à savoir, le ministre de l'Intérieur, pour ce qui concerne les données traitées dans le cadre de la police administrative et le ministre de la Justice, pour les données traitées dans le cadre de la police judiciaire ou conjointement, les deux lorsqu'il s'agit de données traitées dans le cadre de ces deux finalités.

De duidelijke aanwijzing van een verantwoordelijke voor de verwerking is de hoeksteen die toelaat om het hele systeem van uitvoering van de principes van gegevensbescherming, die voor een groot deel rusten op de optie en richtlijnen genomen door de verantwoordelijke voor de verwerking, uit te werken.

De keuze van de voogdijministers voor het beheer van de operationele politie-informatie dwars door de A.N.G. en de gegevensbanken is nodig om, voor het geheel van de geïntegreerde politie, de gestelde keuzes, waaronder de richtlijnen, af te stellen op de voorziene middelen. Men denke bijvoorbeeld aan het toegangsbeheer van de gegevensbanken, aan het beheer en de monitoring van de logging, aan de nadere regels van het bepalen van de evaluatie van verwerkte gegevens, aan de nadere regels van verbinding van gegevensbanken, …

Een decentralisering van de verantwoordelijkheid zou niet meer toelaten om homogeniteit en voorspelbaarheid te garanderen bij een performant informatiebeheer.

Meerdere verwerkingsverantwoordelijken kunnen gezamenlijk gegevens verwerken in een bijzondere gegevensbank waarvoor zij co-verwerkingsverantwoordelijk worden.

Een model van medeverantwoordelijkheid voor de algemene verwerking tussen de politie en de ministers van Binnenlandse Zaken en Justitie, zoals gesuggereerd in punt 8, lid 1, van advies nr. 9/2018 van 12 december 2018 van het Controleorgaan, leidt onvermijdelijk tot een verwatering van de verantwoordelijkheid in de zin van de wet gegevensbescherming tussen de verschillende bevoegdheidsniveaus, hetgeen niet bevorderlijk is voor de doeltreffendheid van de besluitvorming en bijgevolg van de efficiëntie van operationele politiewerkzaamheden.

Dit model werd ook niet gekozen in 2016 voor de gemeenschappelijke gegevensbanken waarin de ministers van Binnenlandse Zaken en Justitie zijn aangewezen als verantwoordelijke voor de verwerking.

In paragraaf 2 wordt ten slotte de zinsnede “en onverminderd de eigen bevoegdheden van de gerechtelijke overheden” verplaatst vanuit het gewijzigde paragraaf 1, dit teneinde de bevoegdheden van de gerechtelijke overheden betreffende de verwerking van gerechtelijke gegevens te behouden.

Op het niveau van het beheer van gerechtelijke politie-informatie, moet natuurlijk ook rekening gehouden worden met de principes van de strafprocedure en in het bijzonder met de principes van het geheim van informatie en van het onderzoek, waarvoor de gerechtelijke autoriteiten garant staan. De bevoegdheid van de

La désignation claire d’un responsable du traitement est la clef de voute permettant d’articuler tout le système d’application des principes de protection des données, qui reposent en grande partie sur les options et les directives prises par les responsables du traitement.

Le choix des ministres de tutelle pour la gestion de l’information policière opérationnelle à travers la B.N.G. et les banques de données de base s’impose afin d’aligner pour l’ensemble de la police intégrée les choix posés, notamment par directives, relatifs aux moyens à mettre en œuvre. On peut penser par exemple à la politique d’accès aux banques de données, à la gestion et au monitoring des journaux, aux modalités de détermination de l’évaluation des informations traitées, aux modalités d’interconnexions de banques de données, …

Une décentralisation de la responsabilité ne permettrait plus d’assurer une homogénéité et une prévisibilité inhérentes à une gestion d’information performante.

Plusieurs responsables du traitement peuvent traiter conjointement des données dans une banque de données particulière, dont ils deviennent co-responsables du traitement

Un modèle en coresponsabilité de traitement généralisé entre la police et les Ministres de l’Intérieur et de la Justice tel que suggéré au point 8, alinéa 1er, de l’avis de l’Organe de contrôle n° 9/2018 du 12 décembre 2018 amènerait inévitablement une dilution de la responsabilité au sens de la loi relative à la protection des données entre différents niveaux de pouvoirs, ce qui n’est pas un élément favorable à l’effectivité des prises de décisions et donc par corrélation à l’efficacité du travail policier opérationnel.

Ce n’est d’ailleurs pas ce modèle non plus qui a été choisi en 2016 lors de la création des banques de données communes où les Ministres de l’Intérieur et de la Justice sont désignés responsables du traitement.

Au paragraphe 2, les mots “et sans préjudice des compétences propres des autorités judiciaires” sont déplacés depuis le paragraphe 1er modifié, afin de maintenir les compétences des autorités judiciaires en matière de traitement de données judiciaires.

Au niveau de la gestion d’information policière judiciaire, il faut bien entendu aussi tenir compte des principes de procédure pénale et en particulier des principes du secret de l’information et de l’instruction dont les autorités judiciaires sont les garantes. C’est dans ce sens qu’il faut comprendre que la compétence

minister van Justitie moet in die zin begrepen worden, onverminderd de bevoegdheid van de gerechtelijke autoriteiten.

Artikel 44/4, § 2, tweede lid, preciseert enerzijds de draagwijdte van de logbestanden en anderzijds de waarborgen inzake veiligheid en integriteit van de logginggegevens alsook inzake de toegang tot de logbestanden. Die bestanden zijn geen kopie van de met de uitgevoerde verwerkingen verrijkte "actieve" databank. Ze stemmen echter overeen met een lijst die toelaat verslag uit te brengen over de verschillende uitgevoerde verwerkingen van de gegevens van de verschillende entiteiten vervat in een gegevensbank.

De definitie en de draagwijdte van de logbestanden is vastgelegd in artikel 56 van de wet gegevensbescherming, maar vond de wetgever het verkieslijk de definitie op te nemen in de WPA (Tucht zie uitleg Richtlijn).

Wanneer de logbestanden van de verwerkingen in de operationele politionele gegevensbanken worden aangemaakt, moeten deze het in principe niet enkel mogelijk maken om de categorie te identificeren van de persoon die de verwerkingen heeft uitgevoerd, maar ook om de persoon zelf te identificeren die de bedoelde verwerkingen heeft uitgevoerd. Het kan gaan om een rechtstreekse identificatie wanneer de identiteit van een personeelslid van de politiediensten rechtstreeks in de logbestanden wordt geregistreerd of via een door de politiediensten gekende gebruikersnaam die toelaat een persoon met een code te verbinden (bijvoorbeeld via een stamnummer) of onrechtstreeks wanneer een individuele cijfercode wordt toegekend aan de persoon die de gegevens verwerkt (bijvoorbeeld raadpleegt) in het geval dat zijn echte identiteit moet worden beschermd. In dat laatste geval zijn enkel de oorspronkelijke dienst van die persoon en de bevoegde toezichthoudende autoriteit uiteindelijk in staat een natuurlijke persoon te identificeren.

Wanneer echter gegevens uit diezelfde gegevensbanken aan een ontvanger worden bezorgd, dan is de identificatie van die ontvanger slechts mogelijk wanneer het gaat om een duidelijk geïdentificeerde natuurlijke persoon. Als die communicatie of die overdracht een rechtspersoon of een technische "*single point of contact*" (SPOC) betreft, belast met de dispatching binnen zijn organisatie, dan zullen de logbestanden van de politie slechts een spoor van de verzending naar die rechtspersoon of die technische SPOC bevatten. In dat geval moet die ontvanger natuurlijk de vereiste technische en organisatorische maatregelen nemen en moet

du ministre de la Justice s'exerce, sans préjudice de la compétence des autorités judiciaires.

L'article 44/4, § 2, alinéa 2, précise d'une part la portée des fichiers de journalisation et, d'autre part, les garanties en matière de sécurité et d'intégrité des données de journalisation ainsi que l'accès aux fichiers de journalisation. Ces derniers ne sont pas une copie de la banque de donnée "active" enrichie des traitements effectués mais ils correspondent à un répertoire qui permet de rendre compte des différents traitements effectués sur des données des différentes entités contenues dans une banque de données.

La définition et la portée des fichiers de journalisation est prévue à l'article 56 de la loi protection des données mais il a semblé préférable au législateur de reprendre la définition dans la LFP (Discipline voir les considérants de la Directive).

Lorsqu'il s'agit d'établir des journaux relatifs aux traitements effectués dans les banques de données policières opérationnelles, ceux-ci doivent en principe permettre non seulement d'identifier la catégorie de personne qui a réalisé les traitements mais aussi d'identifier la personne qui a réalisé les traitements visés. Il peut s'agir d'une identification directe dans le cas où l'identité d'un membre du personnel des services de police est directement enregistrée dans les journaux ou via un identifiant unique, connu des service des police qui permet de relier une personne à un code (par exemple via un numéro de matricule) ou indirecte dans l'hypothèse où un code chiffré individuel est attribué à la personne qui traite (par exemple consulte) les données dans l'hypothèse où son identité réelle doit être protégée. Dans ce dernier cas, seul le service d'origine de cette personne et l'autorité de contrôle compétente sont alors capables *in fine* d'identifier une personne physique.

Cependant, lorsque des données issues de ces mêmes banques de données sont transmises vers un destinataire, l'identification de ce destinataire n'est possible que lorsqu'il s'agit d'une personne physique clairement identifiée. Si cette communication ou ce transfert concerne une personne morale ou "un *single point of contact* technique" (SPOC), chargé d'assurer le dispatching en interne de son organisation, les fichiers de journaux de la police ne contiendront qu'une trace de l'envoi vers cette personne morale ou ce SPOC technique. Il s'agira bien entendu dans ce cas pour ce destinataire de prendre les mesures techniques et

hij bijvoorbeeld op zijn beurt via logbestanden het daaropvolgende gebruik van de gegevens kunnen traceren.

Bijgevolg is duidelijk vastgelegd voor welke verwerkingen logbestanden moeten worden bijgehouden. Die logbestanden mogen slechts worden gebruikt in het kader van de doeleinden bedoeld in artikel 56, § 2, van de wet gegevensbescherming, met name voor de controle van de rechtmatigheid van de verwerking, voor autocontrole, voor het waarborgen van de integriteit en de veiligheid van de persoonsgegevens en voor de doeleinden bedoeld in artikel 27 van dezelfde wet, namelijk voor de voorkoming en opsporing van strafbare feiten, evenals onderzoeken en vervolgingen of de uitvoering van strafrechtelijke sancties, met inbegrip van de bescherming tegen bedreigingen van de openbare veiligheid en de preventie van zulke bedreigingen.

De integriteit van de gegevens van de logbestanden is belangrijk, aangezien die gegevens kunnen dienen om de rechtmatigheid van de uitgevoerde verwerkingen te controleren. Ze kunnen dus dienen als bewijs, bijvoorbeeld in het kader van een strafrechtelijk of tuchtonderzoek wegens onwettige raadpleging van een gegevensbank. Het spreekt dus voor zich dat de systemen technisch zo moeten worden ontworpen dat die integriteit verzekerd wordt.

Tot slot moet er worden voorzien in specifieke procedures voor de toegangen om de noodzaak en de proportionaliteit van de toegangen tot de logbestanden te verzekeren. Die procedures moeten er in het bijzonder voor zorgen dat de logbestanden niet worden gebruikt om de in de WPA vastgelegde bewaartermijnen van de gegevens te omzeilen. Het kan er ook om gaan een rechtvaardiging op te leggen alvorens er toegang toe te hebben. Die procedures houden bovendien in dat een specifiek toegangsprofiel tot de logbestanden wordt geïmplementeerd. Tot slot moeten de personen die de loggingresultaten gebruiken het systeem goed begrijpen om zich ervan te vergewissen dat uit de exploitatie van die gegevens de juiste conclusies worden getrokken.

Het laatste lid wordt aangepast om te preciseren dat de in de WPA en zijn uitvoeringsbesluiten aangewezen beheerders, zoals bijvoorbeeld het geval is voor de gemeenschappelijke gegevensbanken, en de niet-aangewezen beheerders die echter in feite gegevensbanken beheren, toezien op de toepassing van de richtlijnen bedoeld in artikel 44/4, § 2.

De paragraaf 3 wordt ook vervangen en een paragraaf 3*bis* en een paragraaf 3*ter* worden toegevoegd, met als doel om bestaande toepassingen op het terrein, alsook het totaalconcept "*i-Police*", een helder wettelijk

organisationnelles requises et par exemple de pouvoir à son tour tracer via des fichiers de journaux l'utilisation des données qui sera subséquemment réalisée.

Il est de la sorte clairement établi pour quels traitements des fichiers logs doivent être tenus. Les finalités d'utilisation de ces fichiers de journalisation ne peuvent servir que dans le cadre des finalités visées à l'article 56, § 2, de la loi protection des données à savoir à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données à caractère personnel et aux fins visées à l'article 27 de cette même loi, soit 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.

L'intégrité des données des fichiers de journalisation est importante puisque ces données peuvent servir à contrôler la licéité des traitements effectuées et donc servir de preuve, par exemple, dans le cadre d'une enquête pénale ou disciplinaire pour consultation irrégulière d'une banque de données. Il va donc de soi que les systèmes doivent être conçus au niveau technique pour assurer cette intégrité.

Enfin, des procédures spécifiques au niveau des accès doivent être prévues pour assurer la nécessité et la proportionnalité de l'accès aux fichiers de journalisation. Ces procédures doivent notamment assurer que les fichiers de journalisation ne soient pas utilisés pour contourner les durées de conservation des données prévues dans la LFP. Il peut aussi s'agir d'imposer une justification avant d'y accéder. Ces procédures impliquent en outre qu'un profil spécifique d'accès aux fichiers de journalisation soit implémenté. Enfin les personnes qui utilisent les résultats de journalisations doivent avoir une compréhension éclairée du système pour s'assurer que les bonnes conclusions soient tirées de l'exploitation de ces données.

Le dernier alinéa est adapté pour préciser que les gestionnaires désignés dans la LFP et ses arrêtés d'exécution, comme c'est par exemple le cas pour les banques de données communes, ainsi que ceux qui ne sont pas désignés mais qui gèrent, dans les faits, des banques de données veillent en bon père de famille à l'application des directives visées à l'article 44/4, § 2.

Le paragraphe 3 est également remplacé, et un paragraphe 3*bis* et un paragraphe 3*ter* sont ajoutés, afin de donner un cadre légal clair aux applications existantes sur le terrain ainsi qu'au concept total "*i-Police*", en

kader te geven, waarbij naast toegang tot en koppelingen van gegevensbanken ook verdere verwerkingen in deze gegevensbanken mogelijk zijn.

De nieuwe paragraaf 3 bepaalt dat de ministers van Binnenlandse Zaken en Justitie, in hun hoedanigheid van verwerkingsverantwoordelijke, de toegangsregels van de politiediensten tot de politionele gegevensbanken bepalen.

De richtlijnen waarvan sprake in paragrafen 3 en 3*bis* aangaande de toegang tot en de onderlinge koppeling van de bijzondere gegevensbanken en lokale technische gegevensbanken hebben niet als doel om de richtlijnen van de verwerkingsverantwoordelijke(n) te vervangen. Ze kaderen in de verantwoordelijkheden van de ministers om te waken over de geïntegreerde werking van de politiediensten, de informatieveiligheid, het wettelijk kader van de andere gegevensbanken waarvoor zij wel de verwerkingsverantwoordelijken zijn, de regels inzake internationale politiesamenwerking, de federale loyauteit en de wettigheid waarmee bewijsmiddelen worden verzameld. De richtlijnen vormen een kader voor de verwerkingsverantwoordelijken anderen dan de ministers.

Paragraaf 3*bis* neemt de inhoud van de vroegere paragraaf 3 over, deze aanpassend aan de formulering gebruikt voor paragraaf 4, zoals ingevoegd bij de "camerawet" van 21 maart 2018. Deze paragraaf beoogt dus voortaan de koppeling van de gegevensbanken met de verwerkingen die daaruit voortvloeien.

Artikel 44/4 van de WPA was eerder ingevoegd bij wet van 18 maart 2014 om, onder andere, de bevoegde ministers de mogelijkheid te geven de politie op terrein toe te laten de bestaande politionele gegevensbanken onderling met elkaar te kunnen koppelen, alsook met andere gegevensbanken waartoe de politie toegang heeft.

Hoewel de memorie van toelichting van die eerder genoemde wet het niet expliciteert lijkt het niet meer dan logisch dat een koppeling van gegevensbanken enkel nut heeft wanneer men de gekoppelde gegevens eveneens kan verwerken. Het concept van koppeling dekt dus eveneens de daaruit volgende verwerkingen.

De wijzigingen zijn bedoeld om de nodige koppelingen (en verwerkingen) toe te staan voor wat betreft de basisgegevensbanken. Twee politiezones die structureel of occasioneel met elkaar samenwerken (interventie, recherche, slachtofferbejegening …) al of niet in de aanloop van een fusie en gemeenschappelijke patrouilles organiseren kunnen dit bezwaarlijk doen als er operationeel niet de nodige informatie kan vergeleken worden. Eenzelfde benadering is dagelijkse praktijk

permettant également, outre les interconnexions de banques de données, davantage de traitements dans ces banques de données.

Le nouveau paragraphe 3 prévoit que les ministres de l'Intérieur et de la Justice déterminent, en leur qualité de responsables de traitement, les règles d'accès des services de police aux banques de données policières.

Les directives visées aux paragraphes 3 et 3*bis* concernant l'accès aux banques de données particulières et aux banques de données techniques locales, ainsi que leur interconnexion, ne sont pas destinées à remplacer les directives du ou des responsable(s) du traitement. Elles sont prises dans le cadre des responsabilités des ministres en tant que garants du fonctionnement intégré des services de police, de la sécurité de l'information, du cadre légal des autres banques de données dont ils sont responsables du traitement, des règles de coopération policière internationale, de la loyauté fédérale et de la légalité avec laquelle les preuves sont recueillies. Ces directives constituent un cadre pour les responsables de traitement autres que les ministres.

Le paragraphe 3*bis* reprend le contenu de l'ancien paragraphe 3 tout en l'adaptant à la formulation utilisée au paragraphe 4, tel qu'inséré par la loi "caméra" du 21 mars 2018. Ce paragraphe vise donc désormais l'interconnexion de banques de données avec les traitements qui en découlent.

L'article 44/4 de la LFP avait été introduit précédemment par la loi du 18 mars 2014 afin de, notamment, donner aux ministres de tutelle la possibilité de permettre à la police d'interconnecter les banques de données policières sur le terrain, ainsi que d'autres banques de données auxquelles la police a accès.

Bien que l'exposé des motifs de la loi précitée ne le précise pas, il semble logique qu'une interconnexion entre des banque de données ne soit utile que si les données interconnectées peuvent également être traitées. Le concept d'interconnexion implique également les traitements subséquents.

Les modifications visent à permettre aussi d'autoriser les interconnexions (et les traitements) nécessaires en ce qui concerne les banques de données de base. Deux zones de police qui collaborent de façon structurelle ou occasionnelle (intervention, recherche, assistance aux victimes …), que ce soit ou non de façon préalable à une fusion, et organisent des patrouilles communes, peuvent difficilement le faire si elles sont incapables de comparer leurs informations dans le domaine opérationnel.

waar de federale politie via het CIK, de Directie van de openbare veiligheid (DAS) of met andere gespecialiseerde eenheden van bestuurlijke (DAFA, DACH, …) of gerechtelijke politie (de laboratoria van de technische en wetenschappelijke politie), andere entiteiten steun biedt, door het verzekeren van een constante uitwisseling en afstemming van informatie en gegevens binnen een operationeel geïntegreerd politielandschap. Het verzamelen van informatie op de meest actuele en nauwkeurige manier mogelijk om een optimale samenwerking en uitwisseling tot stand te brengen, maakt deel uit van de wettelijke missies van alle geïntegreerde politiediensten. Het is in dit kader (eveneens) van essentieel belang dat deze op een eenvoudige, geïntegreerde en efficiënte wijze ter beschikking worden gesteld van elk lid van de geïntegreerde politiediensten.

Samenwerkingen tussen verschillende korpsen kunnen inderdaad worden gepland in de vorm van een politieassociaties. Een politieassociatie is een overeenkomst waarin afspraken over verregaande samenwerking staan, maar het is geen fusie. Er kan daarbij gedacht worden aan een gezamenlijk bureau APO (Autonoom Politioneel Onderzoek), een gezamenlijke permanentie-officier bestuurlijke politie, gezamenlijke permanentie recherche, dezelfde dienst intern toezicht, enz. Dit heeft tot gevolg dat soms de verschillende korpsen gezamenlijke bijzondere gegevensbanken kunnen opzetten en hierin kunnen verwerken. Eenzelfde noodzaak kan er zijn bij grootschalige evenementen met implicaties voor het grondgebied van verschillende politiezones. In havenzones bijvoorbeeld kunnen er ook samenwerkingen zijn met federale politie. Er kan verwezen worden naar grootschalige projecten zoals “Kanaalplan” en “Stroomplan”.

Verder is het zo dat de politie met de moderne ICT-middelen die er bestaan, op het terrein op een efficiënte wijze informatie moet kunnen verzamelen. Een politieambtenaar kan bijvoorbeeld bij de vaststelling van een verkeersongeval ter plaatse nummerplaten opvragen en gegevens over technische keuring consulteren; bij een vaststelling van een inbraak kan de politie nagaan wie op een bepaald adres woont; bij de identiteitscontrole van een persoon naar aanleiding van een verkeerscontrole of bijstand gerechtsdeurwaarder kan de consultatie van A.N.G. en Rijksregister noodzakelijk zijn; bij een controle van een straatmuzikant kan het noodzakelijk zijn na te gaan of de betrokkene persoon een vergunning van de gemeente heeft; … Al deze bevragingen moeten – uit operationele efficiëntieoverwegingen – door een politiepersoneelslid op het terrein kunnen worden uitgevoerd vanuit “één omgeving”. Indien deze gegevens niet “gekoppeld” worden aangereikt, veronderstelt dit de afzonderlijke consultatie van alle mogelijke gegevensbronnen

Une approche similaire se pratique lorsque la police fédérale agit en appui d’autres entités via le CIK, DAS ou d’autres unités spécialisées de police administrative (DAFA, DACH, …) ou judiciaire (labo), en assurant une coordination et un échange permanents des informations au sein d’un paysage policier intégré sur le plan opérationnel. La collecte d’informations de la manière la plus actuelle et la plus précise possible pour arriver à une collaboration et une coordination optimale fait partie des missions légales de tous les services de police intégrés. Il est dans ce cadre (également) crucial que celles-ci puissent être mises à la disposition de chaque membre de la police intégrée de manière simple, intégrée et efficiente.

Des collaborations entre plusieurs corps peuvent en effet être prévues sous forme d’associations d’entités de police. Une association d’entités de police est un accord portant sur une coopération poussée, mais qui n’équivaut pas à une fusion. Il peut par exemple s’agir d’un bureau commun pour les EPO (enquêtes policières d’office), d’un officier de permanence commun en matière de police administrative, d’une permanence commune en matière de recherche, d’un service unique de contrôle interne, etc. Cela a pour effet que différents corps peuvent parfois mettre en place des banques de données particulières communes et y effectuer des traitements. Il peut y avoir une même nécessité en cas d’événements de grande envergure ayant des implications sur le territoire de plusieurs zones de police. Dans les zones portuaires, il peut également y avoir des collaborations avec la police fédérale. Il est possible de se référer à des projets à grande échelle tels que “Plan Canal” et “*Stroomplan*”.

La police doit en effet pouvoir collecter des informations sur le terrain avec les outils ICT modernes disponibles, et ce d’une manière et efficiente. Par exemple, lors du constat d’un accident de roulage, un fonctionnaire de police peut contrôler sur place les plaques d’immatriculation et consulter les données relatives au contrôle technique; lors du constat d’une effraction, la police peut vérifier qui habite à une adresse déterminée; lors du contrôle d’identité d’une personne dans le cadre d’un contrôle de circulation ou lors d’une mission d’assistance à un huissier de justice, la consultation de la B.N.G. ou du Registre national peut s’avérer nécessaire; lors du contrôle d’un musicien de rue, il peut s’avérer nécessaire de vérifier si la personne concernée est titulaire d’une autorisation de la commune; … Pour des raisons d’efficience opérationnelle, toutes ces consultations doivent pouvoir être effectuées sur le terrain par un membre des services de police au départ d’un “environnement unique”. Si

waarin de informatie beschikbaar is. Het voortdurend communiceren via radiocommunicatie, kan het radionetwerk zwaar belasten, zeker in crisissituaties. Niet alleen het tijdverlies, maar vooral het risico op hoog kwaliteitsverlies (door te veel afzonderlijke manipulaties) is de basisverantwoording om deze gegevens "geïntegreerd" ter beschikking te stellen. Het koppelen van gegevens uit diverse bronnen (zelfstandig gevalideerd) en de verwerking ervan in een eenvoudig te gebruiken hulpmiddel voor de eindgebruiker, zijn inherent aan het huidige politiewerk, modern, efficiënt en vooral veilig.

Er is namelijk binnen de geïntegreerde politie bepaald om één basistoepassing, "*i-Police*", te ontwikkelen voor zowel de federale politie als de lokale politie waarbij simultaan de diverse gegevensbanken waartoe de politie toegang heeft worden geconsulteerd in functie van een toegewezen profiel.

Het moet bijzonder en uitdrukkelijk worden benadrukt dat de beperkingen en voorwaarden voor het gebruik van eender welk gegeven worden bepaald door de rechten van gebruik zoals die aan ieder personeelslid persoonlijk (in functie van zijn gebruikersprofiel) zijn toegekend in relatie tot de soort gegevensbank die aan de basis kan worden bevraagd. Bijgevolg worden de restricties en bijgevolg ook controlevoorzieningen en -mogelijkheden inzake het gebruik van persoonsgebonden gegevens steeds bepaald in verhouding tot de "brongegevensbank en zijn onveranderlijk vastgelegd voor de gebruiker van de "koppeling". De controle en gebruiksrestricties zijn dus technisch verbonden aan het basisbestand of de basisbron en niet aan de applicatie die het gebruik van de gegevens – via een koppeling of verwerking – uit een gegevensbank faciliteert.

Er werd ook een lid toegevoegd in paragraaf 3*bis* om de twee bevoegde ministers toe te laten te bepalen aan welke criteria (bv. toegangsprofielen in functie van de behoefte van te kennen, beveiliging, ...) een dergelijke koppeling dient te voldoen en alsook te bepalen welke gegevensbanken kunnen worden gekoppeld.

De identificatie van de verschillende koppelingen tijdens de verwerkingen zal gebeuren via het register (zie *infra* artikel 32).

De richtlijnen kunnen ook betrekking hebben op volgende criteria: bijhouden van logbestanden, gegevensbeschermingsbeoordeling, beslissingscriteria inzake

ces données ne peuvent pas être fournies de façon "interconnectée", cela implique la consultation séparée de toutes les sources de données dans lesquelles des informations peuvent être disponibles. La communication permanente par radio, peut représenter une lourde charge pour le réseau radio, en particulier en situation de crise. C'est non seulement la perte de temps, mais surtout le risque d'une importante perte de qualité (en raison de manipulations trop nombreuses) qui justifient de mettre ces données à disposition de manière "intégrée". L'interconnexion de données issues de plusieurs sources (validées de façon autonome) et leur traitement dans un outil facile d'utilisation pour l'utilisateur final, sont inhérents au travail policier actuel, moderne, efficient et, surtout, sûr et sécurisé.

Au sein de la police intégrée, il est en effet prévu de développer une application de base unique, "*i-Police*", destinée aussi bien à la police fédérale qu'à la police locale, qui permettra de consulter simultanément les différentes banques de données auxquelles la police a accès en fonction d'un profil octroyé.

Il convient en particulier de souligner expressément que les restrictions et conditions pour l'usage d'une quelconque donnée sont déterminées par les droits d'utilisation tels qu'ils ont été octroyés personnellement à chaque membre du personnel (en fonction de son profil d'utilisateur) par rapport au type de banque de données pouvant être consulté à la base. Par conséquent, les restrictions, et donc les dispositions et possibilités en matière de contrôle par rapport à l'utilisation de données à caractère personnel sont toujours déterminées vis-à-vis de la "banque de données source" et sont fixées de façon immuable pour l'utilisateur de l'"interconnexion". Le contrôle et les restrictions d'usage sont donc techniquement liés au fichier ou à la source de base, et non à l'application qui facilite l'utilisation des données issues d'une banque de données au moyen d'une interconnexion ou d'un traitement.

Un alinéa a également été inséré dans le paragraphe 3*bis*, afin de permettre aux deux ministres de tutelle de déterminer les critères (p. ex.: octroyer les profils d'accès en fonction des besoins, sécurisation, …) auxquels doit satisfaire une telle interconnexion ainsi que de déterminer quelles banques de données peuvent être interconnectées.

L'identification des différentes interconnexions lors des traitements sera réalisée au travers du registre (voir *infra* article 32).

Les directives peuvent également porter sur les critères suivants: journalisation, évaluation de protection des données, critères décisionnels concernant les

andere bronnen dan de authentieke, en profielen van de consultatiemogelijkheden.

Er wordt ook een lid toegevoegd in paragraaf 3*bis* om het toepassingsgebied van de in de artikelen 3 en 3*bis* genoemde richtlijnen te regelen. Bij de bepaling van de profielen en de toegangsmodaliteiten moet rekening worden gehouden met een aantal factoren, zoals de proportionaliteit van de toegang en de behoefte om die te kennen, het juridische doel van elke verwerking, het al dan niet gevoelige karakter van de gegevens, … Bij deze bepaling zal ook rekening worden gehouden met de evaluatie-elementen uiteengezet in artikel 239 van de wet gegevensbescherming.

Tot slot moeten de verschillende toegangen tot de politionele al dan niet gekoppelde gegevensbanken op basis van de principes van *privacy by design* of *by default* zo worden ontworpen dat de geëvalueerde en gevalideerde gegevens duidelijk zichtbaar worden en prioritair kunnen worden geëxploiteerd. Dit is bijzonder belangrijk bij controles die een impact kunnen hebben op de rechten en vrijheden van de personen.

Uiteraard kan het noodzakelijk zijn bij politietussenkomsten waarvan het doel bestaat uit het identificeren van de betrokkenen, het controleren op wapenbezit of andere gelijkaardige veiligheidskwesties, dan wel het nagaan of een onderzoek moet worden ingesteld, bijvoorbeeld tijdens controles langs de weg, of tijdens regelmatige steekproefsgewijze controles wanneer de identiteit van een verdachte of beklaagde nog niet is vastgesteld dat er een eerste afweging moet worden gemaakt. In deze gevallen is een niet gevalideerde informatie van belang. Om deze evaluatie te maken moet een politieambtenaar een afweging kunnen maken van alle beschikbare bronnen.

Binnen het kader van hun rol als toezichthoudende autoriteit, hebben de leden van het Controleorgaan en zijn opsporingsdienst onbeperkte toegang tot de verwerkingen die uitgevoerd worden door de politiediensten (zie artikel 244 van de wet gegevensbescherming). Als zodanig kunnen zij kennis nemen van toegangsprofielen en op de hoogte zijn van de lijst van personeelsleden die een toegang beschikken.

Om een zekere mate van voorzienbaarheid en rechtszekerheid te verzekeren, is de Raad van State in zijn advies 65.312/2 van 4 maart 2019 over dit artikel van oordeel dat een delegatie van de wet aan de ministers belast met de verwerking enkel kan worden uitgevoerd door middel van een koninklijk besluit. Zoals de Raad van State in zijn advies aangeeft, kan de Koning zelf deze opdrachten rechtstreeks delegeren aan de ministers verantwoordelijk voor de verwerking, wat hij inzake

sources autres qu'authentiques et profils des possibilités de consultation.

Afin d'encadrer la portée des directives visées à l'article 3 et 3*bis*, un paragraphe 3*ter* est inséré. La détermination des profils et des modalités d'accès doit tenir compte d'un ensemble de facteurs tels la proportionnalité de l'accès et le besoin d'en connaître, la finalité légale de chaque traitement, la sensibilité ou non des données, … Les éléments d'évaluation fixés à l'article 239 de la loi relative à la protection des données seront également en compte dans cette détermination.

Enfin, sur la base des principes du *privacy by design* ou *by default*, les différents accès aux banques de données policières qu'elles soient interconnectées ou non doivent être conçus de sorte que les données évaluées et validées apparaissent de manière claire et puissent être exploitées prioritairement. Ceci est particulièrement important dans des situations de contrôle pouvant avoir des effets sur les droits et libertés des personnes.

Il va de soi qu'il peut être nécessaire de bien juger si une vérification doit être faite lors d'interventions policières dont le but consiste à identifier des personnes, de contrôler la détention d'armes ou d'autres questions de sécurité de cette nature. C'est une première évaluation qui doit être faite, par exemple, dans le cas d'un contrôle sur la voie publique ou de contrôles aléatoires lorsque l'identité d'un suspect ou d'un inculpé n'est pas encore établie. Dans ces cas, une information non validée est importante. Pour faire son évaluation, le fonctionnaire de police doit pouvoir prendre en compte toutes les sources disponibles.

Dans le cadre de leur mission d'autorité de contrôle, les membres de l'Organe de contrôle et de son service d'enquête ont un accès illimité aux traitements effectués par les services de police (cfr article 244 de la loi relative à la protection des données). À ce titre, ils peuvent consulter les profils d'accès et avoir connaissance de la liste des membres du personnel disposant d'un accès.

Pour assurer un niveau de prévisibilité et de sécurité juridique, le Conseil d'État estime dans son avis 65.312/2 du 4 mars 2019 à propos du présent article qu'une délégation de la loi vers les ministres responsables du traitement ne peut s'opérer que par le truchement d'un arrêté royal. Comme le Conseil d'État l'indique dans son avis, le Roi peut lui-même déléguer ces tâches directement aux ministres responsables du traitement, ce qu'il fera sans aucun doute en la matière puisque tant les accès

ongetwijfeld zal doen aangezien zowel de toegang tot als de koppeling van de gegevensbanken rechtstreeks onder de bevoegdheid van de verwerkingsverantwoordelijken vallen.

Het gebruik van een koninklijk besluit biedt dus geen specifieke voorzienbaarheid of rechtszekerheid. Het is daarom niet nodig in te gaan op deze opmerking van de Raad van State.

Artikel 8 (wijziging artikel 44/5)

De bepaling 7° wordt in eerste instantie toegevoegd aan artikel 44/5, § 1, omdat de nieuwe privacyregels opleggen dat de categorieën van persoonsgegevens dienen te worden gedefinieerd.

De bepaling 7° doelt op de bestuurlijke maatregelen die door een bevoegde bestuurlijke autoriteit ten aanzien van een persoon of een inrichting worden genomen, en door de politiediensten moeten gecontroleerd en opgevolgd worden krachtens de wet. Het gaat dan concreet om onder meer, maar niet exclusief, de beslissingen genomen door de bestuurlijke politieoverheden (de minister van Binnenlandse Zaken, de gouverneur of de burgemeester) in het kader van specifieke wetgeving zoals de Nieuwe Gemeentewet (artikelen 129, 134-135), de Wet van 24 februari 1921 betreffende het verhandelen van giftstoffen, slaapmiddelen en verdovende middelen, psychotrope stoffen, ontsmettingsstoffen en antiseptica en van de stoffen die kunnen gebruikt worden voor de illegale vervaardiging van verdovende middelen en psychotrope stoffen. (artikel 9*bis*), de Dierengezondheidswet van 24 maart 1987 (maatregelen ter voorkoming en bestrijding van de dierenziekten, zoals bijvoorbeeld het instellen van een schutskring ter voorkoming van de verspreiding van de Afrikaanse varkenspest), maar ook om sancties die door andere bevoegde overheden worden genomen, bijvoorbeeld in het kader van de wet van 24 juni 2013 betreffende de gemeentelijke administratieve sancties (schorsing of intrekking van een toestemming of vergunning, tijdelijke of definitieve sluiting van een inrichting) of de voetbalcel van de FOD Binnenlandse Zaken (administratief stadionverbod, administratief perimeterverbod, tijdelijk verbod het grondgebied te verlaten) in het kader van de wet van 21 december 1998 betreffende de veiligheid bij voetbalwedstrijden (voetbalwet).

Het is immers niet meer dan logisch dat de politie de gegevens met betrekking tot deze personen mag verwerken in de basisgegevensbanken en de A.N.G. en deze kan raadplegen indien zij de naleving van deze maatregelen ook effectief moet kunnen opvolgen en afdwingen.

que l'interconnexion des banques de données sont des thématiques qui relèvent directement des compétences des responsables du traitement.

Le recours à un arrêté royal n'offrira donc aucune prévisibilité ou sécurité juridique spécifique. Il n'y a donc pas lieu de suivre cette remarque du Conseil d'État.

Article 8 (modification article 44/5)

La disposition 7° est avant tout insérée à l'article 44/5, § 1er, parce que les nouvelles règles en matière de protection des données imposent de définir les catégories de données à caractère personnel.

La disposition visée au 7° porte sur les mesures administratives prises par une autorité administrative compétente à l'égard d'une personne ou d'un établissement, à l'égard desquelles les services de police doivent assurer un contrôle et un suivi en vertu de la loi. Il s'agit concrètement entre autres, mais pas exclusivement, des décisions prises par les autorités de police administrative (le ministre de l'Intérieur, le gouverneur ou le bourgmestre) dans le cadre de législations particulières telles que la nouvelle loi communale (articles 129, 134-135), loi du 24 février 1921 concernant le trafic des substances vénéneuses, soporifiques, stupéfiantes, psychotropes, désinfectantes ou antiseptiques et des substances pouvant servir à la fabrication illicite de substances stupéfiantes et psychotropes (article 9*bis*), la loi du 24 mars 1987 relative à la santé des animaux (mesure visant à prévenir et à combattre des maladies animales, comme la mise en place d'une zone de protection censée empêcher la propagation de la peste porcine africaine), mais également de sanctions prises par d'autres autorités compétentes, par exemple dans le cadre de la loi du 24 juin 2013 relative aux sanctions administratives communales (suspension ou retrait d'une autorisation ou d'un permis, fermeture temporaire ou définitive d'un établissement) ou par la cellule Football du SPF Intérieur (interdiction administrative de stade, interdiction administrative de périmètre, interdiction temporaire de quitter le territoire) dans le cadre de la loi du 21 décembre 1998 relative à la sécurité lors des matches de football (loi football).

Il est en effet parfaitement logique que la police puisse traiter les données relatives à ces personnes dans les banques de données de base et la B.N.G., et puisse consulter ces banques de données dans la mesure où elle doit également pouvoir suivre et contrôler effectivement le bon respect de ces mesures.

Om te antwoorden op punt 9 van het advies van het Controleorgaan, is de wettelijke basis die de politie toelaat om de eenvoudige administratieve sancties vast te stellen, niet de wet op het politieambt maar wel de wetten, decreten of ordonnanties die daarop betrekking hebben. De door de politie met het oog hierop gerealiseerde verwerking beperkt zich tot de vaststelling ervan. Anderzijds kan de politie ze vaststellen in haar verwerkingsmiddelen maar dient ze te wissen zodra de verzending naar de sanctionerende ambtenaar is gerealiseerd.

Paragraaf 3, 8°, wordt tevens aangevuld, dit door de toevoeging van bijkomende verwijzingen naar bijzondere categorieën van personen vermeld in het Wetboek van strafvordering.

De bedreigde getuigen, diens gezinsleden en andere bloedverwanten behoorden reeds tot de categorieën van personen wiens gegevens in het raam van gerechtelijke politie konden verwerkt worden (artikel 102, 1° tot 3° Sv.). Het wetsvoorstel voegt nu twee nieuwe categorieën toe, met name de categorie van informanten (artikel 47*decies*, § 1, Sv.) en de categorie van burgerinfiltranten (artikel 47*novies*/1, § 1, Sv.). Hierdoor wordt de mogelijkheid voor de politiediensten om de persoonsgegevens van deze personen te verwerken in het kader van de uitvoering van hun opdrachten van gerechtelijke politie onmiskenbaar in de wetgeving vastgelegd.

Tevens is in paragraaf 6 een zinsnede ingevoegd ("niet langer juist zijn"), om gevolg te geven aan artikel 28, 4°, van de wet gegevensbescherming, aangezien dit voordien niet afdoende duidelijk was op juridisch vlak.

Paragraaf 7 van artikel 44/5 heeft betrekking op de persoonsgegevens die verwerkt worden in de basisgegevensbanken, maar die ook, naargelang van het operationele belang om ze te centraliseren, in de A.N.G. kunnen worden verwerkt. Het betreft:

— personen die zich burgerlijke of benadeelde partij hebben gesteld;

— burgerlijk aansprakelijke personen.

Er zal dus niet systematisch een gecentraliseerde verwerking van die gegevens zijn, maar enkel in specifieke gevallen zoals hieronder vermeld.

Deze paragraaf wordt ingevoerd om reden dat het noodzakelijk kan zijn de informatie te verzamelen van personen die zich burgerlijk partij hebben gesteld. Zo kan een klacht zijn neergelegd met burgerlijke partijstelling (bijvoorbeeld voor een geval van huishoudelijk

Pour répondre au point 9 de l'avis de l'Organe de contrôle, la base légale qui permet à police de constater les sanctions administratives simples n'est pas la loi sur la fonction de police mais bien les lois, décret ou ordonnances y relatifs. Le traitement réalisé par la police à cet effet se limite à les constater. Par ailleurs, la police peut les constater dans ses outils de traitements mais elle doit les effacer dès lors que l'envoi est réalisé vers le fonctionnaire sanctionnateur.

Le paragraphe 3, 8°, est également complété par l'ajout de références supplémentaires à certaines catégories de personnes mentionnées dans le Code d'instruction criminelle.

Les témoins menacés, les membres de leur famille et d'autres proches appartiennent déjà aux catégories de personnes dont les données peuvent être traitées à des fins de police judiciaire (art. 102, 1° à 3° CIC). La proposition de loi ajoute à présent deux nouvelles catégories, à savoir la catégorie des indicateurs (article 47*decies*, § 1er, CIC) et la catégorie des infiltrants civils (article 47*novies*/1, § 1er, CIC). Cet ajout consolide dans la loi la possibilité offerte aux services de police de traiter les données à caractère personnel de ces personnes dans le cadre de l'exercice de leurs missions de police judiciaire.

Le paragraphe 6 est également adapté (par l'ajout des termes "ne sont plus exactes") pour donner suite à l'article 28, 4°, de la loi relative à la protection des données, dans la mesure où cet élément manquait jusqu'à présent de clarté sur le plan juridique.

Le paragraphe 7 de l'article 44/5 porte sur les données à caractère personnel qui sont traitées dans les banques de données de base, mais qui peuvent également, en fonction de l'intérêt opérationnel à les centraliser, être traitées dans la B.N.G.. Il s'agit des:

— personnes qui se sont constituées partie civile ou des personnes lésées;

— personnes civilement responsables.

Il n'y aura donc pas systématiquement de traitement centralisé de ces données mais uniquement dans des cas ciblés, tels qu'explicités ci-dessous.

Ce paragraphe est introduit considérant qu'il peut être nécessaire de collecter les informations de personnes s'étant constituées partie civile. Une plainte peut ainsi avoir été déposée avec constitution de partie civile (par exemple, pour un cas de violence domestique, un

geweld, seksueel overschrijdend gedrag, nabestaanden bij medische fout, ...) rechtstreeks bij het parket, onderzoeksmagistraat of tijdens een strafprocedure van een bestaand dossier waarbij voor verder onderzoek politiediensten worden gevraagd deze persoon te verhoren. Het kan daarbij nuttig zijn bij een interventie van de politie, evaluatie van bepaalde informatie of een tegenklacht om deze personen hun identiteit te weten. Dezelfde noodzaak met dezelfde finaliteit doet zich voor wanneer iemand bij de politie een verklaring indient om de hoedanigheid van benadeelde persoon te verkrijgen in de zin van artikel 5*bis* Wet houdende de voorafgaande titel van het wetboek van strafvordering

De tweede categorie van personen bedoeld in paragraaf 7 betreft de rechtspersonen, de bestuurders en zaakvoerders in de zin van het Wetboek van vennootschappen van 7 mei 1999. Rechtspersonen kunnen ook strafrechtelijk verantwoordelijk worden gesteld en, in die hoedanigheid, door de politiediensten worden verhoord. Het is echter niet altijd direct duidelijk welke rol deze personen hebben. Immers, bepaalt artikel 5 *in fine* van het Strafwetboek dat strafrechtelijke verantwoordelijkheid van de rechtspersonen die van de natuurlijke personen, die daders zijn van dezelfde feiten of eraan hebben deelgenomen, niet uitsluit.

Artikel 9 (opheffen onderafdeling)

Aangezien de controle over politionele gegevensbanken (A.N.G., basisgegevensbanken, bijzondere gegevensbanken en technische gegevensbanken) wordt geregeld in het eerder vermelde artikel 71 e.v. van de wet gegevensbescherming, dient dit niet langer bepaald te worden in de WPA.

Voor wat betreft de gemeenschappelijk gegevensbanken, waarbij er een gedeelde verantwoordelijkheid is samen met de inlichtingen- en veiligheidsdiensten, wordt deze controle echter op een aangepaste manier uitgeoefend. Deze regeling werd uiteengezet in de WPA en dit zal het geval blijven, gelet op het specifiek karakter van de gemeenschappelijke gegevensbank, doch dit wordt verplaatst naar het gedeelte van de WPA dat de gemeenschappelijk gegevensbanken regelt (zie artikelen 44/11/3*quinquies*/1 e.v.).

Artikel 10 (wijziging artikel 44/9)

Gelet op de wijzigingen die worden doorgevoerd in artikel 44/5 WPA, dient er eveneens een actualisering te komen betreffende het archiveren van deze gegevens.

comportement sexuel inapproprié, ou encore par les parents proches en cas d'erreur médicale, etc.) directement auprès du parquet, du juge d'instruction, ou au cours d'une procédure pénale dans le cadre d'un dossier existant, où il est demandé aux services de police d'entendre la personne concernée à des fins d'enquête subséquente. Cela peut en outre s'avérer utile dans le cadre d'une intervention de police, de l'évaluation de certaines informations ou d'une contre-plainte afin de connaître l'identité de ces personnes. La même nécessité, avec la même finalité, s'applique lorsque quelqu'un introduit auprès de la police une déclaration en vue d'acquérir la qualité de personne lésée au sens de l'article 5*bis* de la loi contenant le titre préliminaire du Code de procédure pénale.

La seconde catégorie de personnes visée dans ce paragraphe 7 concerne les personnes morales, les administrateurs et gérants au sens du Code des sociétés du 7 mai 1999. Les personnes morales peuvent elles aussi être tenues pénalement responsables, et être, à ce titre, entendues par les services de police. Le rôle que ces personnes revêtent n'apparaît toutefois pas toujours directement avec clarté. L'article 5 *in fine* du Code pénal stipule que la responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs des mêmes faits ou y ayant participé.

Article 9 (abrogation d'une sous-section)

Dès lors que le contrôle des banques de données policières (B.N.G., banques de données de base, banques de données particulières et banques de données techniques) est désormais réglé par les articles 71 et suivants de la loi relative à la protection des données, il ne doit plus faire l'objet de dispositions dans la LFP.

Pour ce qui concerne les banques de données communes, pour lesquelles il existe une responsabilité partagée avec les services de renseignements et de sécurité, ce contrôle est toutefois exercé d'une manière adaptée. Ces dispositions font partie de la LFP et cela restera le cas, étant donné le caractère spécifique de la banque de données commune, mais elles sont déplacées dans la partie de la LFP qui régit les banques de données communes (voir articles 44/11/3*quinquies*/1 s.).

Article 10 (modification article 44/9)

Etant donné les modifications apportées à l'article 44/5 LFP, il convient également d'actualiser les dispositions relatives à l'archivage de ces données.

Doordat er nieuwe categorieën in leven worden geroepen, dienen deze ook opgenomen te worden als te archiveren gegevens. Dergelijke ingreep, hoewel uitermate belangrijk, betreft evenwel een eerder technische aanpassing.

Specifiek met betrekking tot de nieuwe categorie bedoeld in punten 7° (bestuurlijke maatregelen) van artikel 44/5, § 1, werd ervoor gekozen, om de bewaartermijn op generieke wijze op 3 jaar te zetten vanaf de laatste registratie.

Zoals bepaald in artikel 44/9, § 1, tweede lid, wordt de bestuurlijke politiemaatregel die op basis van een beslissing van een bestuurlijke overheid wordt genomen, echter niet gearchiveerd zolang deze actief is, d.w.z. zolang de politie er actief toezicht op moet houden. Het is dus uitdrukkelijk mogelijk om voor bepaalde categorieën van administratieve politiemaatregelen van deze termijn van drie jaar af te wijken.

Teneinde te voldoen aan de verplichting uit de wet gegevensbescherming om een maximale termijn van bewaring van de zogenaamde logbestanden te voorzien, wordt er – naar analogie met de bepaling bij de gemeenschappelijke gegevensbanken – voorzien in een bepaling die deze maximale bewaartermijn specifieert. Voor wat betreft de A.N.G. wordt voorzien in een bewaringstermijn van 30 jaar.

Artikel 11 (wijziging artikel 44/10, § 1)

Elke uitgevoerde raadpleging van de archieven moet eveneens het voorwerp uitmaken van een logbestand dat zal bewaard worden voor een periode van 30 jaar vanaf de aanvang van de bewaartermijn voor de in de A.N.G. uitgevoerde verwerking.

De bewaartermijn van logbestanden is afgestemd op de bewaartermijn van de gegevens waarop deze bestanden mogelijks betrekking hebben. Dit wordt gerechtvaardigd door de noodzaak, om gedurende de hele bewaartermijn van een gegeven te blijven bestaan, om de verwerking die aan de oorsprong van de aanwezigheid van het gegeven binnen de politionele gegevensbanken ligt, evenals de daaropvolgende verwerkingsoperaties waarvan deze het voorwerp was, te kunnen terugvinden. Met andere woorden, het is belangrijk om een spoor van de verzameling van een gegeven te bewaren, ten minste totdat deze wordt gewist.

Comme de nouvelles catégories sont créées, celles-ci doivent également être inclues parmi les données à archiver. Une telle adaptation, bien qu'extrêmement importante, constitue cependant une adaptation plutôt technique.

En ce qui concerne spécifiquement la nouvelle catégorie visée au point 7° (mesures de police administrative) de l'article 44/5, § 1er, le choix a été fait d'appliquer de manière générique le délai de conservation de 3 ans à compter du dernier enregistrement.

Cependant comme le § 1er, alinéa 2, de l'article 44/9 le prévoit la mesure de police administrative prise sur la base d'une décision d'une autorité administrative n'est pas archivée aussi longtemps qu'elle est active c'est-à-dire aussi longtemps que la police doit activement suivre cette mesure. Il est donc possible de manière spécifique de déroger à ce délai de trois ans pour certaines catégories de mesures de police administrative.

Afin de respecter l'obligation imposée par la loi relative à la protection des données de prévoir un délai maximal de conservation des fichiers de journalisation, et par analogie avec la disposition en vigueur pour les banques de données communes, une disposition spécifiant ce délai maximal de conservation est prévue. Pour ce qui concerne la B.N.G., il est prévu un délai de conservation de 30 ans.

Article 11 (modification article 44/10, § 1)

Toute consultation effectuée dans les archives doit également faire l'objet d'une journalisation qui sera conservée pour une période de trente ans à l'instar du délai de conservation pour les traitements effectués dans la B.N.G..

Le délai de conservation des fichiers de journalisation est aligné sur la durée de conservation des données sur lesquelles ces fichiers sont susceptibles de porter. Ceci s'explique par la nécessité de pouvoir retrouver, durant toute la durée de conservation d'une donnée, le traitement à l'origine de la présence de la donnée dans les banques de données policières ainsi que les opérations de traitement subséquentes dont celle-ci a fait l'objet. En d'autres termes, il importe de conserver une trace de la collecte d'une donnée, au moins jusqu'à l'effacement de celle-ci.

Artikel 12 (wijziging artikel 44/11, § 2)

Dit betreft een louter technische aanpassing, waarbij de correcte verwijzing naar het Controleorgaan in de plaats van de gedateerde uitgebreide verwijzing komt.

Artikel 13 (wijziging artikel 44/11/2)

In eerste instantie wordt door het toevoegen van "beheerd" de realiteit juridisch bevestigd. Beheer wil zeggen het up-to-date houden en exploiteren van de ICT-infrastructuren en -applicaties van deze basisgegevensbanken de politionele processen aan te passen van de organisatie om dit te realiseren, ingevolge een wetswijziging of richtlijnen van een politieoverheid zoals instructies en omzendbrieven van het College van procureurs-generaal.

Het kan hier gaan om aanpassingen van de lay-out van de processen-verbaal van verhoor zoals deze bijvoorbeeld noodzakelijk waren ingevolge de verschillende wetswijzigingen naar aanleiding van de Salduzrechtspraak (Europees Hof voor de Rechten van de Mens dd° 20/11/2008 – zie wet tot wijziging van het wetboek van strafvordering en van de wet van 20 juli 1990 betreffende de voorlopige hechtenis, om aan elkeen die wordt verhoord en aan elkeen wiens vrijheid wordt benomen rechten te verlenen, waaronder het recht om een advocaat te raadplegen en door hem te worden bijgestaan), de wetswijziging, onder meer, ingevolge de richtlijn 2013/48/EU van het Europees Parlement en de Raad van 22 oktober 2013 betreffende het recht op toegang tot een advocaat in strafprocedures en in procedures ter uitvoering van een Europees aanhoudingsbevel en het recht om een derde op de hoogte te laten brengen vanaf de vrijheidsbeneming en om met derden en consulaire autoriteiten te communiceren tijdens de vrijheidsbeneming (wet van 21 november 2016 betreffende bepaalde rechten van personen die worden verhoord) alsook de richtlijnen in dat verband door het College van procureurs-generaal (zie onder meer omzendbrief COL 8/2011 inzake de organisatie van de bijstand door een advocaat vanaf het eerste verhoor binnen het kader van het Belgisch strafprocesrecht).

Het eerste lid van paragraaf 2 wordt opgeheven aangezien de toegangsrechten van de leden van de politiediensten tot de basisgegevensbanken, met inbegrip van de basisgegevensbanken die betrekking hebben op het beheer van onderzoeken, thans in artikel 44/4, § 3, en volgende worden geregeld.

Ten slotte wordt er een paragraaf toegevoegd om ook hier tegemoet te komen aan de verplichting om te voorzien in een maximumtermijn voor het bewaren van

Article 12 (modification article 44/11, § 2)

Il s'agit d'une adaptation purement technique, par laquelle la référence correcte à l'Organe de contrôle remplace la référence large qui n'est plus d'actualité.

Article 13 (modification article 44/11/2)

En premier lieu, la réalité est juridiquement confirmée par l'ajout du mot "gérées". "Gestion" signifie tenir à jour et exploiter les infrastructures et les applications ICT de ces banques de données de base ainsi qu'adapter les processus policiers, par exemple à la suite d'une modification législative ou de directives d'une autorité de police, telles que des instructions et circulaires du Collège des procureurs généraux.

Il peut s'agir d'adaptations à la mise en page des procès-verbaux d'audition, telles que rendues nécessaires, par exemple, en raison des différents changements législatifs résultant de la jurisprudence Salduz (Cour européenne des droits de l'homme 20/11/2008 – voy. la loi modifiant le code d'instruction criminelle et la loi du 20 juillet 1990 relative à la détention préventive, accordant des droits à toute personne détenue préventivement et à toute personne auditionnée, dont celui de consulter un avocat et d'être assisté par ce dernier), de la modification législative faisant suite à la directive 2013/48/UE du Parlement européen et du Conseil du 22 octobre 2013 relative au droit d'accès à un avocat dans le cadre des procédures pénales et des procédures relatives au mandat d'arrêt européen, au droit d'informer un tiers dès la privation de liberté et au droit des personnes privées de liberté de communiquer avec des tiers et avec les autorités consulaire (loi du 21 novembre 2016 relative à certains droits des personnes soumises à un interrogatoire) ainsi que des circulaires du Collège des procureurs généraux relatives à cette manière (voy. notamment circulaire COL 8/2011 relative à l'organisation de l'assistance d'un avocat à partir de la première audition dans le cadre de la procédure pénale belge).

L'alinéa 1er du paragraphe 2 est abrogé vu que les droits d'accès des membres des services de police aux banques de données de base, en ce compris les banques de données de base relatives à la gestion des enquêtes, sont dorénavant réglés à l'article 44/4, § 3, et suivants.

Enfin, un paragraphe est ajouté afin de répondre ici également à l'obligation de prévoir un délai maximal pour la conservation des fichiers de journalisation (voir

de logbestanden (zie uiteenzetting bij artikel 10). Er is een bewaartermijn van 15 jaar voorzien, met de mogelijkheid tot een verlenging van die termijn met maximum 15 jaar. Voor de basisgegevensbanken is er dus een minimale bewaartermijn van 15 jaar en een maximale bewaartermijn van 30 jaar.

De bewaartermijn van logbestanden is afgestemd op de bewaartermijn van de gegevens waarop deze bestanden mogelijks betrekking hebben. Dit wordt gerechtvaardigd door de noodzaak, om gedurende de hele bewaartermijn van een gegeven te blijven bestaan, om de verwerking die aan de oorsprong van de aanwezigheid van het gegeven binnen de politionele gegevensbanken ligt, evenals de daaropvolgende verwerkingsoperaties waarvan deze het voorwerp was, te kunnen terugvinden. Met andere woorden, het is belangrijk om een spoor van de verzameling van een gegeven te bewaren, ten minste totdat deze wordt gewist.

Artikel 14 (wijziging artikel 44/11/3)

Het basisartikel voor de bijzondere gegevensbanken wordt met het voorgestelde artikel 14 geherformuleerd, waarbij enerzijds niet langer wordt gesproken over de verwerkingsverantwoordelijkheid, aangezien dit reeds eerder wordt bepaald in artikel 44/4, doch waarbij anderzijds de specificiteit van de bijzondere gegevensbanken toch nog wordt benadrukt.

Teneinde duidelijk aan te geven welke categorieën van persoonsgegevens in de bijzondere gegevensbanken kunnen worden verwerkt, wordt er voorzien in een verwijzing naar artikel 44/5 waar deze categorieën opgesomd zijn.

Het blijft een bijzondere gegevensbank, die niet voor alles kan aangewend worden, doch enkel ingevolge bijzondere behoeften die uiteengezet worden in de memorie van toelichting bij de wet van 18 maart 2014 betreffende het politionele 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, meer bepaald p. 50 en 51:

"*Paragraaf 2 geeft de drie alternatieve beweegredenen aan die de oprichting van een bijzondere gegevensbank kunnen verantwoorden.*

De eerste beweegreden vloeit voort uit de door de politie gevoerde verwerking van de gegevens en de informatie die geclassificeerd zijn in de zin van de wet

commentaire de l'article 10). Il est prévu un délai de 15 ans, avec la possibilité de prolonger ce délai de 15 années supplémentaires au maximum. Pour les banques de données de base, il y a donc un délai minimal de conservation de 15 ans et un délai maximal de conservation de 30 ans.

Le délai de conservation des fichiers de journalisation est aligné sur la durée de conservation des données sur lesquelles ces fichiers sont susceptibles de porter. Ceci s'explique par la nécessité de pouvoir retrouver, durant toute la durée de conservation d'une donnée, le traitement à l'origine de la présence de la donnée dans les banques de données policières ainsi que les opérations de traitement subséquentes dont celle-ci a fait l'objet. En d'autres termes, il importe de conserver une trace de la collecte d'une donnée, au moins jusqu'à l'effacement de celle-ci.

Article 14 (modification article 44/11/3)

L'article 14 en proposition reformule l'article de base relatif aux banques de données particulières, d'une part en n'évoquant plus la responsabilité du traitement, dans la mesure où cet aspect est déjà fixé à l'article 44/4, et d'autre part, en insistant une nouvelle fois sur la spécificité des banques de données particulières.

Afin d'indiquer clairement quelles catégories de données à caractère personnel peuvent être traitées dans les banques de données particulières, une référence est faite à l'article 44/5, qui énumère ces catégories.

Cela demeure une banque de données particulière, qui ne peut pas être utilisée à n'importe quelle fin, mais seulement pour répondre à des besoins particuliers et dans des circonstances exceptionnelles qui sont expliquées dans l'exposé des motifs de la loi du 18 mars 2014 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 des données à caractère personnel et du code d'instruction criminelle, plus précisément p. 50 et 51:

"*Le paragraphe 2 indique les trois conditions alternatives qui peuvent justifier la création d'une banque de données particulière.*

Le premier motif découle du traitement par la police des données ou informations classifiées au sens de la loi du 11 décembre 1998 relative à la classification et

van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen. In de A.N.G. mogen geen geclassificeerde gegevens of informatie geregistreerd worden omdat de A.N.G. niet gehomologeerd werd door de Nationale Veiligheidsoverheid en bovendien, omdat enkel een minderheid van de politiemensen over een veiligheidsmachtiging beschikt. De gegevens betreffende fenomenen zoals het terrorisme of het groot banditisme of de gegevens die komen van diensten die op meer systematische wijze met een classificatiegraad werken, zoals de inlichtingendiensten of de buitenlandse politiediensten, moeten echter door de politiediensten in gegevensbanken kunnen verwerkt worden: bijzondere gegevensbanken zijn dus noodzakelijk.

De tweede beweegreden van de oprichting van een bijzondere gegevensbank vloeit voort uit het feit dat de A.N.G. een algemene gegevensbank moet blijven, dit wil zeggen dat de erin vervatte gegevens begrijpbaar en bijgevolg exploiteerbaar moeten blijven voor het geheel van de gebruikers omdat beantwoord dient te worden aan de regel van de deling van de gegevens. In bepaalde precieze gevallen, hebben de experts van de politie meer specifieke gegevens nodig die meer gericht zijn op hun activiteitendomein. Om deze gegevens te verwerken kan een bijzondere gegevensbank voor hen noodzakelijk zijn.

Dit soort gegevensbanken richt zich bijvoorbeeld op de behoeften van de experts inzake kunstzwendel. Wat de schilderijen betreft, kunnen zij de schilder, de naam van het schilderij, zijn formaat, …, dit wil zeggen de voor hen essentiële elementen, vermelden, die niet sprekend zijn voor de niet-ingewijde politiemensen.

De derde beweegreden heeft betrekking op de puur lokale behoeften. De gegevens van deze bijzondere gegevensbanken hebben geen operationele meerwaarde om geregistreerd te worden in de A.N.G. opdat ze exploiteerbeer zouden zijn door de leden van de geïntegreerde politie. Het betreft bijvoorbeeld een gegevensbank met betrekking tot de personen die op vakantie vertrokken zijn en die zich bij de politiediensten kenbaar maken met de vraag om politoneel toezicht op hun onbewoonde woning te houden. De geregistreerde gegevens zijn slechts interessant voor de betrokken politiezone en voor de beperkte duur van de afwezigheid van de burgers. Een ander voorbeeld is een graffitigegevensbank van een lokale politie of nog een gegevensbank die de contactpersonen van de sociale werkers herneemt aan wie de politiediensten de personen mogen doorsturen die in het kader van hun opdrachten met hen in contact komen."

aux habilitations, attestations et avis de sécurité. La B.N.G. n'est pas la banque de données dans laquelle des données ou informations classifiées peuvent être enregistrées puisque la B.N.G. n'est pas homologuée par l'Autorité Nationale de Sécurité et que, de plus, seule une minorité des policiers disposent d'une habilitation de sécurité. Cependant, les données concernant des phénomènes tels que le terrorisme ou le grand banditisme ou provenant de services travaillants plus systématiquement avec un degré de classification, comme des services de renseignements ou des services de police étrangers doivent pouvoir être traitées dans des banques de données par les services de police: des banques de données particulières sont donc nécessaires.

Le second motif de création d'une banque de données particulière découle du fait que la B.N.G. est une banque de données qui doit rester généraliste, c'est à-dire que les données qu'elle contient doivent rester compréhensibles et donc exploitables pour l'ensemble des utilisateurs puisqu'il faut répondre à la règle d'une mise en commun des données. Dans des cas précis, les experts de la police, ont besoin de données plus spécifiques, beaucoup plus pointues dans leur domaine d'activité. Une banque de données particulière peut leur être nécessaire pour traiter ces données.

Ce type de banque de données vise par exemple les besoins des experts en trafic d'œuvre d'art. S'il s'agit de tableaux, ils peuvent mentionner l'auteur, le nom du tableau, son format, …, c.-à-d. des données essentielles pour eux mais qui ne parlent pas aux policiers non-initiés.

Le troisième motif vise les besoins purement locaux. Les données de ces banques de données particulières n'ont pas de plus-value opérationnelle à être enregistrées dans la B.N.G. pour être exploitables par les membres de la police intégrée. Il s'agit par exemple d'une banque de données relative aux personnes qui sont parties en vacances et qui se font connaître auprès des services de police pour demander la surveillance policière de leur habitation inoccupée. Les données enregistrées n'intéressent que la zone de police concernée et pour une durée limitée à l'absence des citoyens. Un autre exemple est une banque de données TAG ("graffitis") d'une police locale ou encore une banque de données reprenant les personnes de contact des travailleurs sociaux vers lesquels les services de police peuvent envoyer des personnes qui sont en contact avec eux dans le cadre de leurs missions."

Overeenkomstig de definitie van een verwerking zoals opgenomen in het artikel 26, 2°, van de wet gegevensbescherming, zullen de bijzondere gegevensbanken gebruikt worden voor verwerkingen die niet uitgevoerd kunnen worden in een andere gegevensbankcategorie.

In antwoord op zowel de opmerking van de Raad van State als van het Controleorgaan (punt 12 van zijn advies nr. 9/2018 van 12 december) wordt het begrip van uitzonderlijke omstandigheden vervangen door het begrip van specifieke omstandigheden in die zin dat de oprichting van een bijzondere gegevensbank kan voorzien in basisbehoeften op het gebied van het beheer van operationele politionele gegevens. Zoals hierboven vermeld, zijn deze specifieke omstandigheden in de wet omschreven.

Vervolgens wordt het systeem van verplichte aangifte en adviesaanvraag bij het Controleorgaan, dat een register bijhoudt, afgeschaft, aangezien dit niet in overeenstemming is met het systeem dat opgesteld wordt door de wet gegevensbescherming.

Aangezien er dus geen aangifte bij het Controleorgaan meer wordt gedaan en er op geen advies meer gewacht wordt, terwijl er een operationele behoefte is om een gegevensbank aan te maken of de gegevensbank aan te passen, moet men ervoor zorgen dat het Controleorgaan (dat erop moet toezien dat er geen wildgroei is aan bijzondere gegevensbanken) actief op de hoogte wordt gebracht van het feit dat een bijzondere gegevensbank wordt aangemaakt/aangepast.

Het Controleorgaan wordt op de hoogte gebracht via het register van de verwerkingen van de politiediensten. Het Controleorgaan krijgt een signaal dat een nieuwe bijzondere gegevensbank is aangemaakt of dat een bijzondere gegevensbank is gewijzigd. Op basis van de vermeldingen in het register waardoor het Controleorgaan concreet de nieuwe aanmaak of de aan een bijzondere gegevensbank aangebrachte wijzigingen kan zien, zal het opnieuw contact kunnen opnemen met de betrokken DPO om meer informatie te verkrijgen of ter plaatse controles uit te voeren.

Dit register werd overigens beschouwd als een aanvulling op de aangifte bij de Commissie voor de bescherming van de persoonlijke levenssfeer en teneinde hier toegang toe te verkrijgen, dienden de politiediensten zich specifiek te richten tot het Controleorgaan.

Met betrekking tot voorafgaande verklaringen van bijzondere gegevensbanken, geeft het Controleorgaan zelf in haar advies nr. 9/2018 van 12 december 2018 (punt 12, lid 5) aan dat het een advies zou kunnen

Conformément à la définition d'un traitement telle que reprise à l'article 26, 2°, de la loi relative à la protection des données, les banques de données particulières seront destinées à effectuer des traitements qui ne peuvent être réalisés dans une autre catégorie de banque de données.

Néanmoins, pour répondre tant à la remarque du Conseil d'État qu'à celle de l'Organe de contrôle (point 12 de son avis 9/2018 du 12 décembre), la notion de circonstances exceptionnelles est remplacée par celle de circonstances spécifiques dans le sens où la création d'une banque de données particulières peut répondre à des besoins de base en matière de gestion de l'information policière opérationnelle. Comme énoncé ci-dessus, ces circonstances spécifiques sont circonscrites dans la loi.

Ensuite, le système de déclaration obligatoire et de demande d'avis auprès de l'Organe de contrôle qui tient à jour un registre, est abrogé, car ceci ne correspond plus au système établi par la loi relative à la protection des données.

S'il ne s'agit donc plus de réaliser une déclaration *ad hoc* vers l'Organe de contrôle et d'attendre un avis alors qu'il y a un besoin opérationnel de créer une banque de données ou de l'"aménager", il faut cependant aussi permettre à l'Organe de contrôle qui doit veiller à la non-prolifération des banques de données particulières, d'être activement averti d'une création/modification relative à une banque de données particulière.

Cet avertissement de l'Organe de contrôle sera réalisé via le registre des traitements des services de police. Un signal sera envoyé à l'Organe de contrôle lui indiquant qu'une nouvelle banque de données particulière est créée ou est modifiée. Sur la base des indications du registre qui lui permettront de voir concrètement la création nouvelle ou les modifications apportées à une banque de données particulière, l'Organe de contrôle pourra notamment reprendre contact avec le DPO impliqué pour obtenir plus d'informations ou procéder à des contrôles sur place.

Ce registre était d'ailleurs vu comme un complément à la déclaration à la Commission pour la protection de la vie privée et pour y avoir accès, les services de police devaient spécifiquement s'adresser à l'Organe de contrôle.

Pour ce qui concerne les déclarations préalables des banques de données particulières, l'Organe de contrôle indique lui-même dans son avis n° 9/2018 du 12 décembre 2018 (point 12, alinéa 5) qu'il pourrait

uitbrengen op basis van de rechtstreekse toegang die het in het verwerkingsregister en de alarmfunctie heeft gekregen (het kan actief worden in kennis gesteld wanneer een nieuwe gegevensbank in dit register wordt aangegeven). Zij geeft tevens aan dat veel bijzondere gegevensbanken in feite niet uitzonderlijk zijn in die zin dat ze beantwoorden aan een operationele basisbehoefte en deze verklaringen derhalve geen zeldzaam verschijnsel zullen zijn. Het verkrijgen van goedkeuring middels een afzonderlijke verzending van dit register heeft dan ook geen meerwaarde, zowel op operationeel gebied als op het gebied van gegevensbescherming.

Vanzelfsprekend worden alle velden die het Controleorgaan nodig acht om de controle uit te oefenen over de bijzondere gegevensbestanden opgenomen in dit register.

Teneinde zowel aan de politiediensten als aan het Controleorgaan een permanente globale kijk te geven over het geheel van de verwerkingen die vallen onder titel 2, maar eveneens deze die vallen onder de AVG, wordt één enkel register georganiseerd voor de gehele geïntegreerde politie waarvoor een rechtstreekse toegang voor het Controleorgaan werd georganiseerd (zie *infra* artikel 32).

Daarnaast wordt er tevens bepaald in het artikel dat er een maximale bewaartermijn is voor de logbestanden, dit om dezelfde redenen als deze uiteengezet hierboven. Er wordt voorzien in een minimale bewaartermijn van 10 jaar, met de mogelijkheid dit te verlengen tot een totaalduur van 30 jaar.

De bewaartermijn van logbestanden is afgestemd op de bewaartermijn van de gegevens waarop deze bestanden mogelijks betrekking hebben. Dit wordt gerechtvaardigd door de noodzaak, die de hele bewaartermijn van een gegeven blijft bestaan, om de verwerking die aan de oorsprong van de aanwezigheid van het gegeven binnen de politionele gegevensbanken ligt, evenals de daaropvolgende verwerkingsoperaties waarvan deze het voorwerp was, te kunnen terugvinden. Met andere woorden, is het belangrijk om een spoor van de verzameling van een gegeven te bewaren, ten minste totdat deze wordt gewist.

De bijzondere gegevensbanken omvatten zeer verschillende omstandigheden gaande van een louter lokale behoefte tot het beheer van de gegevens door deskundigen inzake terrorisme.

Deze verscheidenheid betekent dat er variabele bewaartermijnen zijn. Deze hangen af van het type

rendre un avis sur base de l'accès direct qui lui serait fourni dans le registre des traitements et de la fonction alarme (il pourra être activement prévenu lorsqu'une nouvelle banque de données sera déclarée dans ce registre). Il mentionne également que beaucoup de banques de données particulières ne sont en fait pas exceptionnelles dans le sens où elles correspondent à un besoin opérationnel de base et ces déclarations ne seront donc pas un fait rare. Le recours au registre des traitements qui est un outil de base pour la police faciliterait cet envoi. Dès lors, obtenir un aval de l'Organe de contrôle via un envoi séparé de ce registre ne représente pas beaucoup de plus-value tant au niveau opérationnel qu'au niveau de la protection des données.

Il va de soi que l'ensemble des champs que l'Organe de contrôle estime nécessaires pour exercer son contrôle sur les banques de données particulières seront repris dans ce registre.

Afin de permettre tant aux services de police qu'à l'Organe de contrôle d'avoir une vue générale permanente sur l'ensemble des traitements, qu'ils soient effectués sous le couvert du titre 2 ou qu'ils relèvent du RGPD, un seul registre est mis en place pour l'ensemble de la police intégrée et un accès direct est prévu pour l'Organe de contrôle (voir *infra* article 32).

Parallèlement, l'article prévoit également qu'un délai maximal de conservation est d'application pour les fichiers de journalisation, et ce pour les mêmes raisons que celles mentionnées ci-dessus. Un délai minimal de conservation de 10 ans est prévu, avec la possibilité de le prolonger pour atteindre une durée totale de 30 ans.

Le délai de conservation des fichiers de journalisation est aligné sur la durée de conservation des données sur lesquelles ces fichiers sont susceptibles de porter. Ceci s'explique par la nécessité de pouvoir retrouver, durant toute la durée de conservation d'une donnée, le traitement à l'origine de la présence de la donnée dans les banques de données policières ainsi que les opérations de traitement subséquentes dont celle-ci a fait l'objet. En d'autres termes, il importe de conserver une trace de la collecte d'une donnée, au moins jusqu'à l'effacement de celle-ci.

Les banques de données particulières recouvrent des réalités très différentes allant d'un besoin purement local à la gestion des données par les experts en matière de terrorisme.

Cette diversité implique des délais de conservation variables en fonction du type de banque de données

bijzondere gegevensbank in kwestie. Bijgevolg zullen de bewaartermijnen van de logbestanden die noodzakelijk zijn om de doelstellingen uit artikel 56 van de wet gegevensbescherming te bereiken in de praktijk uiteenlopen.

De wetgever heeft echter voorzien in een gemeenschappelijke minimale bewaartermijn van de logbestanden voor alle bijzondere gegevensbanken, namelijk 10 jaar. Die termijn is verlengbaar tot maximaal 30 jaar.

Het is derhalve de taak van iedere verwerkingsverantwoordelijke om op een met redenen omklede wijze de juiste bewaartermijn van de logbestanden vast te leggen, die minimaal 10 jaar en maximaal 30 jaar zal zijn.

Deze motivering zal voortvloeien uit de noodzaak om met behulp van de logbestanden alle tijdens de bewaartermijn van de gegevens uitgevoerde verwerkingen te traceren.

Artikel 15 (wijziging artikel 44/11/3*bis*)

Dit betreft een technische aanpassing, waarbij enerzijds de correcte verwijzing naar het Controleorgaan wordt aangebracht en anderzijds er wordt verwezen naar het *ad hoc* toezichtorgaan voor de gemeenschappelijke gegevensbanken, nu bepaald in het voorgestelde artikel 44/11/3*quinquies*/2.

Aangezien de Gegevensbeschermingsautoriteit niet langer de bevoegde toezichthoudende autoriteit was voor de verwerking van informatie en persoonsgegevens in de gemeenschappelijke databanken zoals bedoeld in artikel 44/2, § 2, was het niet langer gerechtvaardigd om de Gegevensbeschermingsautoriteit een bevoegdheid inzake toe te vertrouwen. De verwijzing naar de Commissie voor de bescherming van de persoonlijke levenssfeer moet derhalve worden vervangen door een verwijzing naar het Controleorgaan op de politionele informatie en het Vast Comité voor de controle van de inlichtingen- en veiligheidsdiensten, bedoeld in artikel 28 van de wet van 18 juli 1991 betreffende de controle van politie- en inlichtingendiensten en het Coördinatieorgaan voor de dreigingsanalyse.

Zoals reeds vermeld, zullen de taken van de veiligheidsconsulent, zoals die voorheen bestond, in de toekomst verder worden uitgeoefend door de DPO. Een aanpassing werd daarvoor uitgevoerd.

particulières visé. Conséquemment, les délais de conservation des fichiers de journaux nécessaires pour atteindre les objectifs visés à l'article 56 de la loi protection des données divergeront dans la pratique.

Le législateur a cependant prévu un délai minimal commun de conservation des fichiers de journaux pour toutes les banques de données particulières, à savoir, 10 ans. Ce délai est prolongeable pour atteindre un maximum de 30 ans.

Il appartient dès lors à chaque responsable du traitement d'établir de manière motivée le juste délai de conservation des fichiers de journaux qui se situera entre un minimum de 10 ans et un maximum de 30 ans.

Cette motivation découlera de la nécessité de pouvoir tracer à l'aide des fichiers de journaux l'ensemble des traitements effectués pendant la durée de conservation des données.

Article 15 (modification article 44/11/3*bis*)

Il s'agit d'une adaptation technique par laquelle, d'une part, la référence correcte est faite à l'Organe de contrôle et, d'autre part, il est fait référence à l'organe de contrôle *ad hoc* pour les banques de données communes, à présent prévu à l'article 44/11/3*quinquies*/2 proposé.

L'Autorité de protection des données n'étant plus l'autorité de contrôle compétente pour les traitements des informations et des données à caractère personnel contenues dans les banques de données communes telles que visées à l'article 44/2, § 2, il n'était plus justifié de confier à la Autorité de protection des données une compétence en la matière. Il y a donc lieu de remplacer la référence à la Commission pour la protection de la vie privée par une référence à l'Organe de contrôle de l'information policière et le Comité permanent de contrôle des services de renseignement et de sécurité, visé à l'article 28 de 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.

Comme déjà indiqué, les tâches du conseiller en sécurité, tel qu'il existait auparavant, seront désormais exercées par le DPO. Une modification est effectuée en ce sens.

Artikel 16 (wijziging artikel 44/11/3*ter*)

Zowel het Controleorgaan (punt 13 van advies nr. 9/2018 van 12 december 2018) als de Raad van State (advies 65.312/2 van 4 maart 2019) wijzen erop dat de wetgever eerder is vergeten rechtstreekse toegang te verlenen aan het Comité I en het Controleorgaan tot de gemeenschappelijke gegevensbanken wanneer zij bij wet gezamenlijk als bevoegde controleautoriteit voor deze gemeenschappelijke gegevensbanken zijn aangewezen. De wijziging van artikel 44/11/ter is bedoeld om dit te verhelpen.

Artikel 17 (invoeging artikel 44/11/3*quinquies*/1)

Dit betreft het overhevelen van de reeds bestaande regelgeving aangaande de aanstelling van de vroegere veiligheidsconsulent, nu de DPO, betreffende de gemeenschappelijke gegevensbanken naar de onderafdeling die erop betrekking heeft.

Voor diens opdrachten wordt verwezen naar de wet gegevensbescherming, doch hier bovenop worden nog enkele bijkomende opdrachten toegewezen, te weten opdrachten die destijds reeds werd uitgevoerd door de veiligheidsconsulent. In antwoord op de opmerking van de Raad van State in advies 65.312/2 van 4 maart 2019 betreffende de inventarisatie van opdrachten, menen de opstellers van dit voorstel dat het wenselijk is dat alle opdrachten expliciet worden geciteerd teneinde elke verwarring te vermijden, gezien de uitbreiding van het profiel van de functie en het overschrijden ervan zonder deze te overlappen.

Het verbod bepaald in de opgeheven bepaling van artikel 44/3, om de consulent voor de veiligheid en de bescherming van gegevens aan te wijzen binnen de entiteit aangewezen als beheerder of operationele verantwoordelijke, is niet hernomen aangezien het geen meerwaarde heeft en voor verwarring zorgt. Inderdaad, is het duidelijk dat de beheerder (DRI) of de operationeel verantwoordelijke (OCAD) van de gemeenschappelijke gegevensbanken als zodanig zijn functie niet kan cumuleren met die van DPO om een belangenconflict te vermijden. Dit verbod was natuurlijk niet van toepassing op de DPO van DRI en OCAD die voor wat hen betreedt genieten van de vereiste onafhankelijkheid. Ook wordt gesteld dat de aangewezen DPO rechtstreeks rapporteert aan de ministers van Binnenlandse Zaken en Justitie.

Article 16 (modification article 44/11/3*ter)*

Tant l'Organe de contrôle (point 13 de l'avis n° 9/2018 du 12 décembre 2018) que le Conseil d'État (avis 65.312/2 du 4 mars 2019) font remarquer que le législateur a précédemment oublié de conférer un accès direct au Comité R et à l'Organe de contrôle aux banques de données communes alors qu'ils sont désignés conjointement par la loi comme autorité de contrôle compétente pour ces banques de données communes. La modification apportée à l'article 44/11/3*ter* a pour but de réparer cet oubli.

Article 17 (introduction article 44/11/3*quinquies*/1)

Il s'agit de transférer la réglementation déjà existante relative à la désignation de l'ancien conseiller en sécurité, maintenant DPO, en ce qui concerne les banques de données communes, dans la sous-section y relative.

En ce qui concerne ses missions, il est fait référence à la loi relative à la protection des données, même si quelques missions supplémentaires sont encore ajoutées, à savoir les missions anciennement exercées par le conseiller en sécurité. En réponse à la remarque du Conseil d'État formulée dans son avis 65.312/2 du 4 mars 2019 concernant l'inventaire des missions, les rédacteurs de la présente proposition estiment qu'il est préférable de citer l'ensemble des missions explicitement afin d'éviter toute confusion vu l'extension du profil de la fonction et le croisement de celles-ci sans se recouper.

L'interdiction, prévue dans la disposition de l'article 44/3 abrogée, de désigner le conseiller en sécurité et en protection des données au sein de l'entité désignée comme gestionnaire ou responsable opérationnel n'a pas été reprise car elle n'a pas de plus-value et porte à confusion. En effet, il est évident que le gestionnaire (DRI) ou le responsable opérationnel (OCAM) des banques de données communes ne peuvent pas cumuler leur fonction avec celle de DPO de la banque de données commune afin d'éviter des conflits d'intérêts. Cette interdiction n'était bien entendu pas applicable aux DPO de DRI ou de l'OCAM qui quant à eux jouissent de l'indépendance requise. Il est d'ailleurs précisé que le DPO qui sera désigné rend compte directement aux ministres de l'Intérieur et de la Justice.

Artikel 18 (invoeging artikel 44/11/3*quinquies*/2)

Hier wordt het vroegere artikel 44/6 deels overgeheveld en wordt er bepaald hoe en door wie er controle wordt uitgeoefend over de gemeenschappelijke gegevensbanken. Het betreft hier evenwel *de facto* een verderzetting van de vorige regeling. Wel werd er een actualisering doorgevoerd en werd – gelet op de definitie van het Controleorgaan – de gebruikte terminologie bijgewerkt.

Article 18 (introduction article 44/11/3*quinquies*/2)

L'ancien article 44/6 est ici partiellement transféré et il est déterminé par qui et comment le contrôle sur les banques de données communes est effectué. Il s'agit toutefois *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 de l'Organe de contrôle.

Artikel 19 (wijziging artikel 44/11/3*septies*, 2°)

Het artikel 44/11/3*septies,* 2°, ingevoegd door de wet van 21 maart 2018 tot wijziging van de wet op het politieambt om het gebruik van camera's door de politiediensten te regelen […] geeft aan welke opdrachten het gebruik van technische gegevensbanken rechtvaardigen en verwijst hierbij naar het artikel 44/5, § 1. Gelet op de uitbreiding van dit artikel met een categorie 7° en het feit dat de inzet van de technische ANPR-gegevensbank nuttig kan zijn en kan bijdragen tot een effectieve en efficiënte inzet van de politiemiddelen bij de controle op de naleving van bestuurlijke maatregelen, is het noodzakelijk om deze bepaling mee op te nemen in onderhavig artikel.

In de praktijk zullen deze bestuurlijke maatregelen veelal beperkt zijn in de tijd (bijvoorbeeld bij een tijdelijke sluiting van een inrichting of naar aanleiding van een administratief stadionverbod, toegepast gedurende de periode van de voetbalwedstrijd) en vaak, doch niet uitsluitend, een lokaal karakter hebben. Deze beperkingen zullen in de gegevensbank worden gematerialiseerd via de criteria tijd, ruimte en frequentie zoals bepaald in het artikel 44/4, § 4, tweede lid. In voorkomend geval kan er echter wel op basis van een beslissing door een bestuurlijke overheid binnen een grotere ruimte worden gewerkt, weliswaar opnieuw beperkt in de tijd voor de duur van de maatregel. Zo kan op efficiënte wijze, in plaats van dagenlang een grootschalige inzet van politie die het vrachtverkeer moet controleren, binnen een bepaalde schutskring een bestuurlijke maatregel worden opgevolgd zoals bijvoorbeeld in het kader van de voorkoming van de verspreiding van de Afrikaanse varkenspest.

Hoewel deze wijziging (verwijzing naar het nieuwe punt 7° van het artikel 44/5, § 1) noodzakelijk is om de finaliteiten vast te leggen die het gebruik van technische gegevensbanken rechtvaardigen, is het niet nodig om dezelfde wijziging aan te brengen in het artikel 25/3, § 2, dat een specifieke hypothese van zichtbaar cameragebruik regelt. Het is immers zo dat het gebruik van zichtbare camera's om feiten vast te stellen die

Article 19 (modification à l'article 44/11/3*septies*, 2°)

L'article 44/11/3*septies*, 2°, inséré par la loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police […] précise les missions justifiant le recours à des banques de données techniques et fait référence dans ce cadre à l'article 44/5, § 1er. Étant donné l'ajout d'une catégorie 7° à cet article et le fait que le recours à la banque de données technique ANPR peut s'avérer utile et peut contribuer à une mise en œuvre efficace et efficiente des moyens policiers dans le cadre du contrôle du respect des mesures administratives, il est nécessaire d'ajouter également cette disposition dans le présent article.

En pratique, ces mesures administratives seront généralement limitées dans le temps (par exemple, en cas de fermeture temporaire d'un établissement ou d'une interdiction administrative de stade appliquée durant la période d'un match de football) et auront souvent, mais pas uniquement, un caractère local. Ces restrictions seront matérialisées dans la banque de données à l'aide des critères de temps, d'espace et de fréquence, tels que prévus à l'article 44/4, § 4, alinéa 2. Le cas échéant, il est toutefois possible de travailler au sein d'un espace plus large sur décision d'une autorité administrative, mais à nouveau dans un laps de temps limité à la durée de la mesure. Ceci permet de contrôler efficacement une mesure administrative, par exemple dans le cadre de la prévention de la propagation de la peste porcine africaine, sans avoir à déployer un engagement policier à grande échelle durant plusieurs jours pour contrôler le trafic de marchandises au sein d'une zone de protection déterminée.

Si cette modification (le renvoi au nouveau point 7° de l'article 44/5, § 1er) s'avère nécessaire pour adapter les finalités permettant de justifier le recours à une banque de données techniques, il n'est pas nécessaire d'effectuer la même modification à l'article 25/3, § 2, qui règle, quant à lui, une hypothèse particulière d'utilisation visible de caméras. En effet, l'utilisation de caméras visibles pour constater des faits passibles

aanleiding kunnen geven tot een administratieve sanctie of voor de opvolging van bestuurlijke of politiemaatregelen, gedekt wordt door het artikel 25/3, § 1, volgens het welke de politiediensten op zichtbare wijze camera's mogen gebruiken "in het kader van hun opdrachten". De memorie van toelichting van de wet van 21 maart 2018 preciseert dat het hier zowel opdrachten van bestuurlijke als gerechtelijke politie betreft (*Parl. St.* Kamer, DOC 54 2855/001, 15). Het artikel 25/3, § 2, van zijn kant viseert de activiteit van de gerichte bestuurlijke informatiegaring ten opzichte van vooraf bepaalde personen. Het gaat in dat geval dus niet over de loutere vaststelling van feiten door een toezichtscamera, maar wel over het inwinnen van informatie. De voormelde memorie van toelichting licht deze nuance toe met de volgende woorden: "Het feit om in het punt 5°, artikel 21 uitgesloten te hebben – dat betrekking heeft op vreemdelingen – verhindert bijvoorbeeld niet dat men, dankzij warmtecamera's bij een controle buitenlandse personen aantreft die illegaal worden vervoerd in een voertuig. Het is wel verboden om camera's te gebruiken om informatie in te winnen over vreemdelingen" (*Parl. St.* Kamer, DOC 54 2855/001, 20).

Artikelen 20 (wijziging artikel 44/11/8) en 21 (invoeging artikel 44/11/8*bis*)

Het OCAD wordt uit artikel 44/11/8 verwijderd en opgenomen in artikel 44/11/8*bis*. Samen met de schrapping van punt 1° van artikel 44/11/9, § 1, dat betrekking heeft op de inlichtingendiensten (zie verder bij de aanpassingen aan artikel 21), betreft het technische wijzigingen die toelaten in één enkel artikel duidelijk geïdentificeerde diensten samen te brengen, met name enerzijds het OCAD en anderzijds de inlichtingendiensten, om hen in artikel 44/11/12 een rechtstreekse toegang tot de A.N.G. te kunnen geven. In se blijft het principe in dit artikel ongewijzigd, aangezien die twee diensten zoals in het verleden de mogelijkheid behouden om alle in het kader van de uitoefening van hun opdrachten relevante gegevens en informatie te krijgen.

Zoals het geval is voor de in artikel 44/11/9, § 1, bedoelde bestemmelingen, behoort het toe aan de ministers van Binnenlandse Zaken en Justitie om de modaliteiten te bepalen voor het meedelen van deze gegevens aan de in artikel 44/11/8*bis* bedoelde bestemmelingen.

Artikel 22 (wijziging artikel 44/11/9)

Deze bepaling bevat drie wijzigingen. De eerste is een technische wijziging en betreft een hernummering

de sanctions administratives ou pour assurer le suivi et le contrôle de mesures de police ou de mesures administratives est visé par l'article 25/3, § 1er, au terme duquel les services de police peuvent utiliser de manière visible des caméras "dans le cadre de leurs missions". L'exposé des motifs de la loi du 21 mars 2018 précise qu'il s'agit ici des missions tant de police administrative que de police judiciaire (*Doc. Parl.* Chambre, DOC 54 2855/1, 15). L'article 25/3, § 2, quant à lui vise l'hypothèse de la récolte d'information de police administrative au sujet de personnes déterminées. Il ne vise donc pas la constatation de faits, mais bien la collecte d'informations. L'exposé des motifs précité illustre cette nuance en ces termes: "Le fait d'avoir, dans le 5°, exclu l'article 21, qui concerne les étrangers n'empêche pas, par exemple, que grâce à des caméras thermiques, l'on détecte que des personnes étrangères sont transportées illégalement dans un véhicule, lors d'un contrôle. Ce qui est interdit, c'est l'utilisation de caméras en vue de recueillir des informations sur les étrangers" (*Doc. Parl.* Chambre, DOC 54 2855/001, 20).

Articles 20 (modification de l'article 44/11/8) et 21 (introduction article 44/11/8*bis*)

L'OCAM est supprimé de l'article 44/11/8 et est inséré à l'article 44/11/8*bis*. Combiné à la suppression du point 1° de l'article 44/11/9, § 1er, qui concerne les services de renseignement (voir *infra* les modifications portées par l'article 21), il s'agit de modifications techniques qui permettent de regrouper dans un seul article deux services clairement identifiés, à savoir d'une part l'OCAM et d'autre part les services de renseignement, afin de pouvoir leur conférer dans l'article 44/11/12 un accès direct à la B.N.G. En soi, le principe reste inchangé dans cet article puisque ces deux services gardent comme par le passé la possibilité de recevoir communication de l'ensemble des données et informations pertinentes dans le cadre de l'exercice de leurs missions.

Comme c'est le cas pour les destinataires visés à l'art. 44/11/9, § 1er, il appartient aux ministres de l'Intérieur et de la Justice de déterminer les modalités de communication de ces données aux destinataires visés à l'art. 44/11/8*bis*.

Article 22 (modification article 44/11/9)

Cette disposition contient trois modifications. La première est une modification technique et consiste en

ingevolge de verplaatsing van de inlichtingendiensten naar het nieuwe artikel 44/11/8*bis*.

De tweede wijziging heeft betrekking op de draagwijdte van het advies van de regelgever dat specifiek betrekking heeft op "Belgische openbare overheden, publieke organen of instellingen van openbaar nut die door de wet belast zijn met de toepassing van de strafwet of die wettelijke verplichten inzake de openbare veiligheid hebben, wanneer deze ze nodig hebben voor de uitvoering van hun wettelijke opdrachten".

Het Controleorgaan verwijst naar het arrest 108/2016 van het Grondwettelijk Hof van 14-07-2016 met het verzoek zijn voorafgaand advies als bindend te beschouwen.

Opgemerkt moet echter worden dat dit arrest van 2016 dateert van vóór de inwerkingtreding van de AVG-regels, waarbij de aandacht van de verantwoordelijke voor de verwerking en de controles achteraf van de gegevensbeschermingsautoriteiten ligt. Een voorafgaande controle door het Controleorgaan op de kwaliteit van deze autoriteiten, organen of organen of gegevensstromen past niet in de filosofie van de AVG en is ook een belemmering voor de optimale stroom van operationele gegevens tussen de partners van de strafrechts- en veiligheidsketen. Om tegemoet te komen aan de wens van het Grondwettelijk Hof voor transparantie, wordt de lijst van overheden, organen of instellingen bedoeld in § 2 van artikel 44/11/9 bepaald door de minister van Binnenlandse Zaken en Justitie. Deze lijst zal worden opgesteld na het niet-bindend advies van het Comité bedoeld in artikel 8*quater*/1 van de wet op de geïntegreerde politie gestructureerd op twee niveaus. Verder worden deze gegevensfluxen ook omkaderd op basis van richtlijnen van de ministers van Binnenlandse zaken en Justitie. Het Controleorgaan oefent in het kader van deze mededelingen, evenals in het kader van deze bedoeld in artikel 44/11/9, § 1, al haar prerogatieven uit om a posteriori de gegevensstromen te controleren.

De derde wijziging betreft paragraaf 3 en wordt ingevoerd aangezien het logischer is dat de verwerkingsverantwoordelijke zelf het protocol afsluit voor deze informatie-uitwisseling. Mogelijks betreft het immers informatie in een bijzondere gegevensbank, waarvan de commissaris-generaal niet de verwerkingsverantwoordelijke is, maar een korpschef. Het is desgevallend aangewezen dat de korpschef dit protocol afsluit.

une renumérotation suite au transfert des services de renseignement vers le nouvel article 44/11/8*bis*.

La deuxième modification concerne la portée de l'avis de l'Organe de contrôle spécifiquement concernant les "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 lorsque ceux-ci en ont besoin pour l'exécution de leurs missions légales".

L'Organe de contrôle fait référence à l'arrêt 108/2016 du 14-07-2016 de la Cour constitutionnelle pour demander que son avis *a priori* soit considéré comme obligatoire.

Il faut cependant constater que cet arrêt de 2016 est antérieur à l'entrée en vigueur des règles du RGPD où l'accent est mis sur la responsabilité du responsable du traitement et les contrôles a posteriori des autorités de protection des données. Un contrôle *a priori* de l'Organe de contrôle quant à la qualité de ces autorités, organes ou organismes ou aux flux de données ne rentre donc pas dans la philosophie du RGPD et constitue en outre un frein à la circulation optimale des données opérationnelles entre les partenaires de la chaîne pénale et de sécurité. Afin de rencontrer le souhait de transparence de la Cour constitutionnelle, la liste des autorités, organes ou organismes visés au § 2 de l'article 44/11/9 est déterminée par le ministre de l'Intérieur et de la Justice. Cette liste sera élaborée après l'avis bien entendu non contraignant du Comité visé à l'article 8*quater*/1 de la loi relative à la police intégrée structurée à deux niveaux. En outre, les flux de données sont encadrés par des directives des ministres de l'Intérieur et de la Justice. L'Organe de contrôle exerce dans le cadre de ces communications, comme d'ailleurs dans le cadre de celles visées à l'article 44/11/9, § 1er, toutes ses prérogatives de contrôle a posteriori des flux de données.

La troisième modification concerne le paragraphe 3 et est introduite dans la mesure où il est logique que le responsable du traitement conclut lui-même le protocole relatif à cet échange de données. Il peut en effet s'agir d'informations dans une banque de données particulière pour lesquelles le responsable du traitement n'est pas le commissaire général, mais un chef de corps. Dans ce cas, il est indiqué que le chef de corps conclue ce protocole.

Artikel 23 (wijziging artikelen 44/11/10 en 44/11/11)

Aangezien de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit een hervorming heeft doorgevoerd inzake de opdrachten van de Commissie voor de bescherming van de persoonlijke levenssfeer en gelet op artikel 71 van de wet gegevensbescherming die het Controleorgaan bevoegd maakt voor de controle over politionele informatieverwerking, was het niet langer gerechtvaardigd dat de Commissie voor de bescherming van de persoonlijke levenssfeer/ Gegevensbeschermingsautoriteit nog adviserend zou optreden in politionele materies. Teneinde te antwoorden op het Controleorgaan (advies nr. 009/2018 van 12 december 2018) en zoals hierboven aangegeven, is de toewijzing van de rol van het Controleorgaan als Sectoraal Comité geen doelstelling van de wetgever.

Article 23 (modification articles 44/11/10 et 44/11/11)

Dans la mesure où la loi du 3 décembre 2017 portant création de l'Autorité de protection des données a réformé les missions de la Commission de la protection de la vie privée, et en application de l'article 71 de la loi relative à la protection des données, qui rend l'Organe de contrôle compétent en matière de contrôle des traitements d'informations par la police, il n'était plus justifié de confier à la Commission de la protection de la vie privée/Autorité de protection des données un rôle consultatif dans les matières policières. Pour répondre à l'Organe de contrôle (avis n°009/2018 du 12 décembre 2018), et comme indiqué *supra*, l'attribution du rôle de Comité sectoriel à l'Organe de contrôle n'est pas un objectif voulu par le législateur.

Artikel 24 (wijziging artikel 44/11/12, § 1)

Artikel 44/11/12 werd aangepast om de inlichtingendiensten een rechtstreekse toegang tot de A.N.G. te geven.

De rechtstreekse toegang tot de A.N.G. is een belangrijk punt voor de correcte uitvoering van de wettelijke opdrachten die de inlichtingen en veiligheidsdiensten zijn toevertrouwd.

In het algemeen moeten de inlichtingen en veiligheidsdiensten, om hun opdrachten te kunnen uitvoeren, haar organieke wet, en in het bijzonder het artikel 14, zo efficiënt mogelijk kunnen aanwenden.

Bepaalde politiegegevens en -informatie die vervat zijn in de A.N.G. zijn van essentieel belang voor de inlichtingen en veiligheidsdiensten voor de uitvoering van hun opdrachten op het gebied van bescherming, detectie, preventie en de belemmering van dreigingen voor de "nationale veiligheid" of voor de Staat, of het nu gaat om terrorisme of spionage en inmenging.

De dreigingen die de inlichtingen en veiligheidsdiensten opvolgen, vinden immers vaak hun oorsprong in strafbare feiten of bedreigingen voor de openbare orde, waar de Politie verwijzing van maakt in de A.N.G. en anderzijds kunnen die bedreigingen een impact hebben op de veiligheid/de openbare orde.

De politie-informatie kan voor de inlichtingen en veiligheidsdiensten dus het vertrekpunt zijn van een

Article 24 (modification article 44/11/12, § 1er)

L'article 44/11/12 a été adapté pour permettre un accès direct de la B.N.G. au profit des services de renseignement.

L'accès direct à la B.N.G. est un point important pour la correcte réalisation des missions légales dévolues aux services de renseignement et de sécurité.

De manière générale, pour pouvoir réaliser leurs missions, les services de renseignement et de sécurité doivent pouvoir mettre en œuvre leur loi organique, et en particulier son article 14, de la manière la plus efficace possible.

Certains types de données et informations policières contenues dans la B.N.G. sont essentielles aux services de renseignement et de sécurité pour réaliser leurs missions de protection, de détection, de prévention et d'entrave des menaces à la "sécurité nationale" ou à l'État, qu'il s'agisse de terrorisme ou d'espionnage et d'ingérence.

En effet, les menaces sur lesquelles travaille les services de renseignement et de sécurité trouvent souvent leurs prémisses dans des faits infractionnels ou de menaces à l'ordre public, référencés par la Police dans la B.N.G. et d'autre part, ces menaces peuvent avoir un impact potentiel sur la sécurité/l'ordre public.

L'information policière peut donc pour les services de renseignement et de sécurité, signifier le point de départ

inlichtingenonderzoek binnen domeinen waar er een gedeelde verantwoordelijkheid is (bv. terrorisme of extremisme).

Voor wat betreft de inlichtingenonderzoeken, vormt de politie-informatie overigens ook een onontbeerlijke bron van historische contextuele informatie, in de vorm van gerechtelijke en administratieve antecedenten van individuen of persoonsgegevens, aan de hand waarvan men de informatie uit het inlichtingenwerk kan aanvullen, een antwoord kan bieden op de onderzoeksvragen voor de identificatie en lokalisatie van personen (bijvoorbeeld wanneer persoon x op plaats x werd bekeurd voor overdreven snelheid kan men deze op een precies tijdstip lokaliseren), verbanden kan leggen tussen deze personen en hun activiteiten kan vaststellen, om zo te beoordelen of deze een bedreiging vormen in de zin van artikel 8 en van 11 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (WIV) en om de politieke, administratieve en gerechtelijke besluitvorming te ondersteunen.

Vanuit methodologisch oogpunt bepalen de finaliteiten van de inlichtingen en veiligheidsdiensten dat de formulering van onderzoekshypotheses in het begin zeer breed is en dan steeds beperkter wordt doorheen de selectie van gegevens bij elke fase van de onderzoeksvraagstelling om potentiële targets en dreigingen te detecteren. Voor de inlichtingen en veiligheidsdiensten wordt de proportionaliteit beoordeeld aan de hand van het gebruik van de gegevens en de selectie ervan doorheen de verschillende fases van het onderzoek. Het is deze selectie van relevante gegevens, binnen de context van het onderzoek, die door de inlichtingen en veiligheidsdiensten met de grootst mogelijke discretie moet worden behandeld.

Het feit dat de politiegegevens essentieel zijn voor de uitoefening van de opdrachten van de inlichtingen- en veiligheidsdiensten is ongetwijfeld de reden waarom het principe van de toegang tot deze politiegegevens voor de inlichtingen- en veiligheidsdiensten sinds 2014 is vastgelegd in de WPA en sinds 2010 in de WIV.

Ondanks het feit dat de noodzaak erkend wordt, staat de huidige manier van informatiemededeling niet op punt en de oproep in de aanbevelingen van de Parlementaire Onderzoekscommissie “Aanslagen” om de uitwisseling van informatie te verbeteren, moet op deze manier worden opgevat.

Hoewel de uitwisseling van informatie tussen de politiediensten en de inlichtingendiensten constant is, gebeurt deze nu immers aan de hand van *ad hoc*-mechanismen via formele tussenpersonen zoals de twee verbindingsofficieren van de VSSE bij de

d’une enquête de renseignement dans des domaines où il y a notamment une responsabilité partagée (ex. terrorisme ou extrémisme).

Par ailleurs, l’information policière constitue pour les enquêtes de renseignement une information contextuelle historique indispensable des antécédents judiciaires et administratifs concernant des individus ou des données à caractère personnel permettant d’enrichir les informations du renseignement et de répondre aux questions investigatives visant à identifier des personnes, à les localiser (par exemple, tel individu a été verbalisé à tel endroit pour un excès de vitesse permet de le localiser à un moment précis), d’établir des liens entre elles et de définir leurs activités en vue d’évaluer si elles représentent une menace au sens de l’article 8 et de l’art. 11 de la Loi organique des services de renseignement et de sécurité du 30 novembre 1998 (LRS) et d’aider à la prise de décisions politiques, administratives et judiciaires.

D’un point de vue méthodologique, les finalités des services de renseignement et de sécurité impliquent que la formulation d’hypothèses de recherche est au départ très large et se restreint progressivement au travers de la sélection de données à chaque étape du questionnement investigatif pour détecter des targets et des menaces potentielles. Pour les services de renseignement et de sécurité, c’est sur l’utilisation des données, leur sélection, au fil des étapes de la recherche qu’est évaluée la proportionnalité. C’est cette sélection de données pertinentes, dans le contexte de la recherche, qui doit être traitée par les services de renseignements et de sécurité avec la plus grande discrétion.

Il est tellement évident que les données policières sont essentielles à l’exécution des missions des services de renseignement et de sécurité que le principe de l’accès à ces données policières pour les services de renseignement et de sécurité est inscrit dans la LFP depuis 2014 et dans la LRS depuis 2010.

Toutefois, si le besoin est reconnu, la forme actuelle de la communication des données n’est pas idoine et l’appel de la Commission d’enquête parlementaire “attentats” dans ses recommandations d’améliorer le partage d’informations doit être comprise dans ce sens.

En effet, actuellement, bien que les échanges d’informations entre les services de police et les services de renseignement soient constants, ils sont réalisés par des mécanismes *ad hoc* au travers de relais formels comme les deux officiers de liaison VSSE auprès de

Federale Politie of de verbindingsofficier van ADIV, of via de contacten die op gezette tijden plaatsvinden tussen onderzoekers binnen concrete dossiers of naar aanleiding van werkplatforms (zoals onder meer de LTF's en de werkgroepen van het Plan R), of via de mechanismen voor technische bijstand, of via informele akkoorden over de systematische overdracht van bepaalde documenten via e-mail (bijvoorbeeld RIR/RAR inzake terrorisme), maar ook vaak op vraag van een onderzoeker van de inlichtingen en veiligheidsdiensten die zijn of haar onderzoeksvraag voorlegt aan een gesprekspartner bij de politie, die vaak op geografische of thematische basis wordt gekozen. Ook al zijn deze uitwisselingen talrijk, zijn ze niet gestandaardiseerd en genormaliseerd. Ze gaan ze vaak enkel over dossiers waarin er een samenwerking bestaat, laten ze niet echt toe om transversale verbanden te leggen. Ze vereisen talrijke manuele verrichtingen, en doen bijgevolg beroep op veel menselijke middelen. Op het vlak van veiligheid (discretie van de onderzoeken) en bescherming van de gegevens (minimalisering) noodzaken deze uitwisselingen nog maatregelen om te beantwoorden aan de verplichting tot traceerbaarheid en aan de nieuwe wettelijke verplichtingen inzake de bescherming van inlichtingenonderzoeken, bronnen en identiteit van agenten die onder andere geregeld worden in de wet op de gegevensbescherming.

Aangezien de inlichtingen en veiligheidsdiensten voor hun opdrachten niet rechtstreeks toegang hebben tot alle relevante politie-informatie, zien zij zich genoodzaakt om op ongeschikte wijze het opzoekwerk, d.w.z. de selectie van de gegevens, van een investigator van de inlichtingen en veiligheidsdiensten – in principe als enige bekleed met deze opdracht – toe te vertrouwen/te delegeren/over te dragen aan mogelijkerwijs verschillende gesprekspartners van de Politie die elk een deel van de kennis/toegang hebben al naargelang hun rol ten opzichte van het onderwerp van het onderzoek, met een onzeker resultaat wat betreft het relevant karakter.

Bovendien biedt de mededeling van gegevens de inlichtingen en veiligheidsdiensten niet de mogelijkheid om zich te baseren op politie-informatie en deze volledig te benutten in het inlichtingenkader als contextuele basis om mogelijke dreigingen op te sporen en nieuwe onderzoeken op te starten.

Daarom is het om redenen van efficiëntie bij de opsporing van dreigingen, van veiligheid, van besparing, van verrijking en coördinatie, en om het vermoeden van onschuld en het recht op respect van de privacy te behouden, noodzakelijk dat een geautomatiseerde rechtstreekse toegang tot de A.N.G. aan de inlichtingen en veiligheidsdiensten toegekend wordt.

la Police fédérale, ou l'officier de liaison de SGRS ou de contacts ponctuels entre enquêteurs dans des dossiers concrets ou à l'occasion de plateformes de travail (comme entre autres, les LTF et les groupes de travail du Plan R) ou via les mécanismes d'assistance technique ou d'accords informels pris sur la transmission systématique de certains documents sous format mail (par exemple, RIR/RAR en matière de terrorisme), mais souvent aussi à la demande d'un enquêteur des services de renseignement et de sécurité qui transmet sa question investigative à un interlocuteur policier, choisi souvent sur base géographique ou thématique. Si ces échanges sont nombreux, ils ne sont pas standardisés et normalisés. Ils ne concernent souvent que des dossiers où une collaboration existe et permettent difficilement de faire des liens transversaux. Ils requièrent de nombreuses opérations manuelles et par conséquent mobilisent beaucoup de ressources humaines. En termes de sécurité (discrétion des recherches) et de protection des données (minimisation), ces échanges nécessitent en outre des mesures afin de répondre aux obligations de traçabilité et aux nouvelles obligations légales de protection des enquêtes, des sources et de l'identité des agents de renseignement prévues entre autres par la loi relative à la protection des données.

En n'ayant pas accès direct à l'ensemble des informations policières pertinentes pour leurs missions, les services de renseignement et de sécurité se voient forcés de confier/déléguer/transférer de manière inadéquate la recherche, c'est-à-dire la sélection des données, d'un investigateur des services de renseignement et de sécurité – en principe, seul à être investi de cette mission – à potentiellement de multiples interlocuteurs de la Police qui détiennent chacun une partie de la connaissance/de l'accès, en fonction de leur rôle par rapport à l'objet de l'enquête, avec un résultat incertain en ce qui concerne la pertinence.

Par ailleurs, la communication de données ne permet pas aux services de renseignement et de sécurité de s'appuyer sur les informations policières et de les valoriser pleinement dans le cadre renseignement comme base contextuelle pour détecter des menaces potentielles et initier des enquêtes nouvelles.

C'est pourquoi, pour des raisons d'efficacité dans la détection des menaces, de sécurité, d'économie, d'enrichissement et de coordination, et pour préserver la présomption d'innocence et le droit au respect de la vie privée, il est nécessaire qu'un accès direct automatisé à la B.N.G. soit accordé aux services de renseignement et de sécurité.

In functionele termen zal deze rechtstreekse toegang het mogelijk maken dat de gegevens en informatie uit de A.N.G., in samenhang met de inlichtingengegevens, het zullen toelaten om formeel een entiteit (bijvoorbeeld een persoon) te identificeren, banden van deze entiteit met andere entiteiten te definiëren en haar gevaarlijkheid uit te leggen.

Binnen dezelfde optiek werd bovendien de rechtstreekse toegang tot de gegevens van het ANPR reeds ingevoerd in de WIV door artikel 16/4.

Rekening houdend met deze technologische mogelijkheden moet het principe van rechtstreekse toegang tot de politiegegevens het mogelijk maken om tot oplossingen te komen die de functionele eisen m.b.t. de finaliteiten van opzoeking en analyse van de inlichtingen en veiligheidsdiensten verenigen met de verplichtingen van veiligheid en bescherming van de gegevens die zowel aan de Politie als aan de inlichtingendiensten opgelegd zijn.

De technische modaliteiten van de beveiligde toegang worden in onderlinge overeenstemming tussen de Politie en de inlichtingen en veiligheidsdiensten uitgewerkt en in een protocol geformaliseerd.

De toegang tot politiegegevens is beperkt tot bepaalde agenten van inlichtingen en veiligheidsdiensten, houder van de veiligheidsmachtiging van het niveau Zeer Geheim en waarvan de profielen gedefinieerd zijn met specifieke rechten gelinkt aan hun opzoekingsopdrachten.

Het geheel van deze maatregelen maakt het dus mogelijk om technisch te garanderen dat de politiegegevens die toegankelijk gemaakt zijn voor de inlichtingen en veiligheidsdiensten, beschermd worden, van a tot z te traceren en te controleren zijn, zoals vereist door de wet op de gegevensbescherming.

Wat de wederkerigheid betreft, volgen de inlichtingen en veiligheidsdiensten volledig de lijn van de meest efficiënt mogelijke gegevensuitwisseling met de Politie, met naleving van de wederzijdse verplichtingen en de principes van goede samenwerking zoals deze al zijn opgenomen in de artikelen 19 en 20 WIV.

Dit betreft in de eerste plaats grondige uitwisselingen waarbij het één van de finaliteiten van de inlichtingen en veiligheidsdiensten moet zijn om de politiegegevens te valoriseren, benutten en verrijken met het oog op het opsporen en verminderen van de dreigingen. Door de politiegegevens in perspectief te plaatsen met behulp van de geclassificeerde gegevens afkomstig van de nationale of internationale inlichtingenvergaring, zullen

En termes fonctionnels, cet accès direct permettra notamment, en corrélant les données du renseignement avec celles contenues dans la B.N.G., d'identifier formellement une entité (par exemple, une personne), de définir les liens de cette entité avec d'autres entités et d'expliquer sa dangerosité.

C'est dans cette même optique que l'accès direct aux données des ANPR a par ailleurs déjà été introduit par l'article 16/4 dans la LRS.

Compte tenu des possibilités technologiques, le principe de l'accès direct aux données policières doit permettre de dégager des solutions alliant les exigences fonctionnelles liées aux finalités de recherche et d'analyse des services de renseignement et de sécurité ainsi que les contraintes de sécurité et de protection des données qui sont imposées à la fois à la police et aux services de renseignement.

En ce qui concerne les modalités techniques, l'accès sécurisé est réalisé de commun accord entre la police et les services de renseignement et de sécurité et est formalisé dans un protocole.

L'accès aux données policières est toutefois limité à certains agents des services de renseignements et de sécurité, titulaires de l'habilitation de sécurité de niveau Très Secret et dont les profils sont définis avec des droits spécifiques liés à leurs missions de recherche.

Toutes les mesures sont prises afin de garantir techniquement que les données policières rendues accessibles aux services de renseignements et de sécurité sont protégées, traçables de bout en bout et auditables, comme l'exige la loi relative à la protection des données.

En ce qui concerne la réciprocité, les services de renseignement et de sécurité s'inscrivent totalement dans une logique d'échange le plus efficace possible avec la Police, dans le respect des contraintes mutuelles et des principes de bonne coopération tels qu'inscrits déjà dans la LRS en ses articles 19 et 20.

Ceci concerne en premier lieu les échanges de fond où une des finalités des services de renseignement et de sécurité doit être de valoriser, exploiter et enrichir les données policières en vue de réaliser sa mission de détection et de réduction des menaces. En mettant en perspective les données policières à l'aide des données classifiées issues de la collecte nationale ou internationale du renseignement, les services de renseignement

de inlichtingen en veiligheidsdiensten in staat zijn om terug te keren naar de Politiediensten met solide hypothesen die hefbomen kunnen zijn voor acties van de administratieve en gerechtelijke politie.

Dit betekent dat de inlichtingen en veiligheidsdiensten op eigen initiatief gegevens meedelen aan de Politie en dat ze tegelijkertijd een antwoord geven op de vragen om informatie van de Politie op de meest gepaste manier, weze het via een toegang of elke andere vorm van mededeling van gegevens, zoals aanbevolen in de artikelen 19 en 20 WIV.

Om dit punt in een concreet jasje te gieten zullen de modaliteiten voor de mededeling aan de Politie in een protocolakkoord vastgelegd worden. Dit protocol treedt in werking gelijktijdig met de directe toegang van de inlichtingen en veiligheidsdiensten tot de A.N.G..

De rechtstreekse toegang tot de databanken met politiegegevens, waaronder deze van de A.N.G., is een belangrijk punt voor de correcte uitvoering van de wettelijke opdrachten die de inlichtingen en veiligheidsdiensten zijn toevertrouwd.

De opstellers van dit voorstel willen graag de volgende aanvullende informatie verstrekken met betrekking tot de rechtstreekse toegang van de inlichtingendiensten tot de Algemene Nationale Gegevensbank (punt 14, advies 009/2018 van 12 december 2018 van het Controleorgaan van de politionele informatie).

Ten eerste, met betrekking tot de behoefte aan een rechtstreekse toegang tot de A.N.G. en niet een rechtstreekse bevraging, is het noodzakelijk om te onthouden dat de rechtstreekse bevraging een model is in de vorm van een HIT (bekende entiteit) / NO HIT (entiteit niet bekend) met, in het geval van HIT een beetje aanvullende informatie in het gegeven antwoord. Dit laat de inlichtingendiensten niet toe om hun wettelijke opdrachten op bruikbare wijze te vervullen. Het HIT/NO HIT-model is inderdaad hoofzakelijk een binair model. De A.N.G. wordt bevraagd over een entiteit (bijvoorbeeld een persoon, een nummer of een plaat) en men ontvangt alleen een (gedeeltelijk) antwoord voor die entiteit. Wat de inlichtingendiensten nodig hebben om hun opdrachten correct te kunnen vervullen, is een weergave van het relationele model dat ten grondslag ligt aan de constructie van de A.N.G., d.w.z. alle verbanden tussen de entiteiten te zien (zien dat een bepaald persoon is gerelateerd aan bepaalde feiten en dat deze feiten gerelateerd zijn aan andere personen, die verder bekend zijn en gerelateerd zijn aan informatierapporten). Alleen de rechtstreekse toegang tot de A.N.G. biedt op een gemakkelijke manier toegang tot dit relationele model. Doordat men directe toegang verleent, is het

et de sécurité seront en mesure de retourner vers les services de Police avec des hypothèses solides qui peuvent être des leviers à des actions de police administrative et judiciaire.

Cela signifie à la fois que des données sont communiquées d'initiative par les services de renseignement et de sécurité à la Police et qu'ils répondent aux demandes d'informations formulées par la Police et ce, sous la forme la plus adaptée, que ce soit via un accès ou toute autre forme de communication de données, comme le recommandent les articles 19 et 20 de la LRS.

Afin de concrétiser ce point, un protocole d'accord déterminera les modalités de communication vers la police. Ce protocole entrera en vigueur simultanément à l'accès direct des services de renseignement et de sécurité à la B.N.G..

L'accès direct aux banques de données comportant des données policières, dont celles figurant dans la B.N.G., est un point important dans l'optique de l'exécution correcte des missions légales confiées aux services de renseignement et de sécurité.

Les rédacteurs de la présente proposition souhaitent apporter les précisions suivantes quant à l'accès direct des services de renseignement à la Banque de données Nationale Générale (point 14 avis 009/2018 du 12 décembre 2018 de l'Organe de contrôle).

Premièrement, pour ce qui concerne la nécessité de conférer un accès direct à la B.N.G. et non une interrogation directe, il s'agit de rappeler que l'interrogation directe est un modèle sous la forme d'un HIT (entité connue)/NO HIT (entité pas connue) avec en cas de HIT un peu d'informations complémentaires dans la réponse fournie. Ceci ne permet pas aux services de renseignement de remplir utilement leurs missions légales. En effet, le modèle de HIT/NO HIT est essentiellement un modèle binaire. On interroge la B.N.G. à propos d'une entité (une personne, un numéro, une plaque, par exemple) et on reçoit une réponse (partielle) uniquement pour ladite entité. Ce dont les services de renseignement ont besoin pour pouvoir remplir correctement leurs missions, c'est une vue sur le modèle relationnel qui est sous-jacent à la construction de la B.N.G. c'est-à-dire voir l'ensemble des liens entre les entités (voir que telle personne est en lien avec tels faits et que ces faits sont en liens avec d'autres personnes, qui par ailleurs sont connues et liées à des rapports d'informations). Seul un accès direct à la B.N.G. permet aisément d'accéder à ce modèle relationnel. Il ne s'agit bien entendu pas en conférant un accès direct de mettre les services de renseignement sur le même pied que les

natuurlijk niet zo dat men de inlichtingendiensten op gelijke voet plaatst met de gerechtelijke overheid of de administratieve politie. Immers, de rechtstreekse toegang tot de A.N.G., verandert de reikwijdte van de wettelijke opdrachten van de inlichtingendiensten niet, maar maakt het simpelweg mogelijk om hun te geven wat ze nodig hebben om deze zo goed mogelijk uit te oefenen.

Ten tweede heeft het Controleorgaan twijfels over de evenredigheid van de rechtstreekse toegang voor inlichtingendiensten. Echter, we moeten vaststellen dat in het raam van dossiers rond terrorisme, radicalisme en extremisme, ... het noodzakelijk is om, in overeenstemming met de A.N.G. beheersregels, alle antecedenten van een persoon te kennen, van de meest onschuldige tot de ernstigere, ten einde zich een beeld te vormen van de gevaarlijkheid van de persoon of om het te onderzoeken (bijvoorbeeld een PV verkeer op een bepaalde datum en plaats, betekent dat deze wagen, die op naam van deze persoon is geregistreerd, zich op die dag op die plaats bevindt). De wetgever heeft gewenst dat de inlichtingendiensten op een verkennende manier kunnen werken (ze zijn niet zoals de politie aan overtredingen gebonden) en daarom is het logisch dat ze alles kunnen zien van de A.N.G.. Het is dan aan de inlichtingendiensten om vervolgens te selecteren en het is niet operationeel verdedigbaar dat deze selectie vooraf wordt gedaan. Het is eveneens belangrijk te noteren dat de rechtstreekse toegang enkel over de A.N.G. handelt en niet over alle informatie van de politiediensten (geen toegang tot bijvoorbeeld de basisgegevensbanken). Deze directe toegang maakt geen inbreuk uit op het vermoeden van onschuld, aangezien zoals hoger aangegeven, de inlichtingendiensten uiteraard in het kader van hun wettelijke taken werken met een verkennend model: het is aldus niet zo dat iemand die het voorwerp uitmaakt van een onderzoek door de inlichtingendiensten, deze persoon ook schuldig is. Wat de inmenging in de persoonlijke levenssfeer betreft, hetgeen een consultatie in de gegevensbanken ook is, betreft een transversaal onderwerp voor alle consultaties en dit is niet eigen aan louter inlichtingendiensten.

Ten derde voor wat betreft de wederkerigheid, deze zal behandeld worden door de verantwoordelijk voor de verwerkingen met de steun van de betrokken diensten en in het passende rechtsinstrument worden opgenomen. In overeenstemming met de regels voor de verdeling van de bevoegdheden tussen de verschillende toezichthoudende autoriteiten voor gegevensbescherming, zal dit rechtsinstrument worden voorgelegd voor advies aan het Vast Comité voor de controle van de inlichtingendiensten. Kortom, het is de behoefte om te kennen die de toegang tot gegevens leidt.

autorités judiciaires ou de police administrative. En effet, l'accès direct à la B.N.G. ne change en rien la portée des missions légales des services de renseignement mais permet simplement de leur donner ce dont ils ont besoin pour les exercer au mieux.

Deuxièmement, l'Organe de contrôle a des doutes quant à la proportionnalité d'un accès direct pour les services de renseignement. Cependant, force est de constater que dans le cadre des dossiers relatifs au terrorisme, au radicalisme et à l'extrémisme, … il est nécessaire de connaître, dans le respect des règles de gestion de la B.N.G., tous les antécédents d'une personne, du plus anodin, au plus grave pour se former une image de la dangerosité de la personne ou pour enquêter sur elle (par exemple un PV de roulage tel jour à tel endroit signifie que la voiture immatriculée au nom de cette personne se trouve tel jour à tel endroit). Le législateur a voulu que les services de renseignement puissent travailler de manière exploratoire (ils ne sont pas tenus comme la police à des infractions) et c'est donc logique qu'ils puissent tout voir en ce qui concerne la B.N.G.. C'est aux services de renseignement qu'il appartient ensuite de faire le tri et il n'est pas opérationnellement défendable que ce tri soit fait préalablement. Il est aussi important de noter que l'accès direct ne porte que sur la B.N.G. et pas sur toute l'information des services de police (il n'y a par exemple pas d'accès direct possible pour les banques de données de base). Cet accès direct ne constitue pas une violation de la présomption d'innocence puisque comme mentionné *supra*, les services de renseignement travaillent, bien entendu dans le cadre de leurs missions légales, avec un modèle exploratoire: ce n'est donc pas parce qu'une personne fait l'objet de recherche de la part de services de renseignement qu'elle est coupable. En ce qui concerne l'immixtion dans la vie privée que constitue une consultation d'une banque de données, c'est une question transversale à toutes les consultations et elle n'est pas propre aux services de renseignement.

Troisièmement, en termes de réciprocité, celle-ci sera traitée entre les responsables du traitement avec l'appui des services concernés et sera coulée dans l'instrument juridique adéquat. Conformément aux règles de répartition de compétence entre les différentes autorités de contrôle compétentes en matière de protection des données, cet instrument juridique sera soumis préalablement à l'avis du Comité permanent de contrôle des services de renseignement. De manière fondamentale, c'est bien le besoin d'en connaître qui guide l'accès aux données.

Ten vierde maakt het Controleorgaan bezwaar tegen het rechtsinstrument dat zal worden gebruikt om deze communicatie van gegevens van de inlichtingendiensten naar de politie operationeel te maken, namelijk, een protocolakkoord. In de mate dat het protocolakkoord geen juridisch instrument is die enkel in deze materie wordt gebruikt, gaat het niet over een uitzondering: zowel de kaderwet voor gegevensbescherming (artikel 20) als de wet op de politieambt (artikel 44/11/9) voorzien eveneens in de verstrekking van gegevens op basis van een protocolakkoord.

Ten vijfde, deze directe toegang is in de feiten en wat betreft het nagestreefde doel redelijk beperkt: het betreft maar enkele honderden leden van inlichtingendiensten, bovendien, houders van een veiligheidsmachtiging en werkzaam rond zware bedreigingen zoals gedefinieerd in de organieke wet, terwijl de A.N.G. reeds toegankelijk is voor verschillende tienduizenden politiemensen.

Ten slotte stelt de Raad van State (advies 65 312/2 van 4 maart 2019) dat er aan moet worden herinnerd dat wanneer toegang aan andere overheidsinstanties wordt verleend, er moet worden nagegaan of de finaliteit van de gegevensbank wel degelijk overeenkomt met de wettelijke opdrachten van alle betrokken overheidsinstanties.

De doelstellingen van de A.N.G. zijn bepaald middels artikel 44/7 van de wet op het politieambt. Deze doelstellingen zijn vervat in deze die zijn opgenomen in artikel 27 van de wet gegevensbescherming (de doelstellingen van de richtlijn 2016/680). Een verdere behandeling voor andere doeleinden (namelijk deze van de inlichtingen) is toegestaan op basis van artikel 29, § 2, van de kaderwet inzake gegevensbescherming.

Dit lid bepaalt dat “de persoonsgegevens niet verder verwerkt kunnen worden door dezelfde of een andere verwerkingsverantwoordelijke voor andere doeleinden dan deze waarvoor de persoonsgegevens werden verzameld, indien dat doeleinde niet ondergebracht kan worden onder de doeleinden vermeld in artikel 27, tenzij deze verdere verwerking is toegestaan overeenkomstig de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst”. Aangezien de wetgever een rechtstreekse toegang (maar principieel is de vraag net dezelfde voor de rechtstreekse bevraging) van de inlichtingendiensten tot de A.N.G. toestaat, kunnen de gegevens van de A.N.G. worden gebruikt voor inlichtingendoeleinden.

Quatrièmement, l’Organe de contrôle émet une objection à l’encontre de l’instrument juridique qui sera utilisé pour opérationnaliser la communication de données des services de renseignement vers la police, à savoir, un protocole d’accord. Dans la mesure où le protocole d’accord n’est pas un instrument juridique utilisé en cette seule matière, il ne s’agit pas d’une exception: tant la loi-cadre protection des données (article 20) que la loi sur la fonction de police (article 44/11/9) prévoient également la communication de données sur base d’un protocole d’accord.

Cinquièmement, cet accès direct est dans les faits et quant à l’objectif poursuivi assez circonscrit: il ne concerne que quelques centaines d’agents des services de renseignement, par ailleurs titulaires d’une habilitation de sécurité, et travaillant sur des menaces graves définies dans la loi organique, alors que la B.N.G. est déjà accessible à plusieurs dizaines de milliers de policiers

Enfin, le Conseil d’État (avis 65.312/2 du 4 mars 2019 indique qu’il y a lieu de rappeler que, lorsqu’un accès est donné à d’autres autorités publiques, il y a lieu de vérifier si les finalités de la banque de données correspondent bien aux missions légales de toutes les autorités publiques concernés.

Les finalités de la B.N.G. sont définies à l’article 44/7 de la loi sur la fonction de police. Ces finalités sont comprises dans celles visées à l’article 27 de la loi protection des données (les finalité de la directive 2016/680). Un traitement ultérieur pour d’autres finalités (à savoir celles de renseignement) est permis sur la base de l’article 29, § 2, de la loi cadre en matière de protection des données.

Ce paragraphe stipule que “les données à caractère personnel ne peuvent pas être traitées ultérieurement par le même ou un autre responsable du traitement à d’autres fins que celles pour lesquelles les données à caractère personnel ont été collectées, et non comprises dans les finalités énoncées à l’article 27, à moins que cette finalité ne soit permise conformément à la loi, au décret, à l’ordonnance, au droit de l’Union européenne ou à l’accord international”. Dès lors que le législateur permet l’accès direct (mais cette question de principe est la même pour l’interrogation directe) des services de renseignement à la B.N.G., il permet que les données de la B.N.G. soient utilisées dans le cadre des finalités de renseignement.

Artikel 25 (wijziging artikel 44/11/13, § 1)

Dit betreft een actualisering en aanpassing aan de nieuwe reglementering, enerzijds qua toepasselijke regelgeving en anderzijds kwestie van het bevoegde adviesorgaan.

Artikel 26 (wijziging artikel 46/1)

Dit betreft een technische aanpassing, gelet op de wijzigingen aan de definitie en de rechtsgrond van het Controleorgaan.

HOOFDSTUK II

Wijzigingen van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus

Artikelen 27-28 (invoeging artikel 8*quater*/1)

Middels deze artikelen wordt er een nieuw adviescomité in het leven geroepen, dat een adviesfunctie zal hebben in het raam van informatieverwerking en -beheer.

De informatieverwerking bij de politiediensten is van zeer groot belang, zowel voor het operationele werk als voor een goed beheer van de organisatie.

Om de verwerkingsverantwoordelijken en de verantwoordelijken voor het beheer van de politiediensten weloverwogen adviezen en aanbevelingen te geven om de informatiesystemen voor te bereiden en te ontwikkelen, wordt een “Adviescomité belast met de strategie inzake informatie en ICT binnen de geïntegreerde politie”, “Comité Informatie en ICT” genaamd, opgericht.

Dit Comité is eveneens gelast met het verlenen van adviezen en formuleren van aanbevelingen inzake informatieveiligheid en bescherming van persoonsgegevens.

Het bestaat uit een gelijk aantal leden van de federale politie en de lokale politie en van vertegenwoordigers van de ministers van Binnenlandse Zaken en Justitie. In antwoord op de opmerking van de Raad van State in zijn advies 65 312/2 van 4 maart 2019, wordt gespecificeerd dat de presidenten leden van de politie zijn. De DPO die is aangewezen bij de Commissaris-generaal of zijn vertegenwoordiger wordt als deskundige betrokken bij

Article 25 (modification article 44/11/13, § 1)

Il s’agit d’une actualisation et d’une adaptation à la nouvelle réglementation, d’abord en ce qui concerne la réglementation applicable, et ensuite en ce qui concerne l’organe consultatif compétent.

Article 26 (modification article 46/1)

Il s’agit d’une adaptation technique, étant donné les modifications apportées à la définition et à la base légale de l’Organe de contrôle.

CHAPITRE II

Modifications de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux

Articles 27-28 (introduction article 8*quater*/1)

Ces articles mettent en place un nouveau comité consultatif qui aura une fonction d’avis dans le cadre du traitement et de la gestion de l’information.

Le traitement de l’information au sein des services de police est un élément d’importance capitale tant pour le travail opérationnel que pour une bonne gestion de l’organisation.

Afin de permettre aux responsables de traitement et aux responsables de la gestion des services de police de recevoir des avis éclairés et des recommandations pour préparer et mettre en place les systèmes d’information, un “Comité d’avis en charge de la stratégie en matière d’information et d’ICT au sein de la police intégrée”, dénommé “Comité Information et l’ICT” est créé.

Ce Comité est également chargé de remettre des avis et des recommandations en matière de sécurité de l’information et de protection des données à caractère personnel.

Il est composé d’un nombre équivalent de membres de la police fédérale et locale et de représentants des ministres de l’Intérieur et de la Justice. En réponse à la remarque du Conseil d’État formulée dans son avis 65.312/2 du 4 mars 2019, il est précisé que les présidents font partie des membres de la police. Comme expert, le DPO désigné auprès du Commissaire général, ou son représentant, est associé aux travaux, en

de werkzaamheden, in het bijzonder voor de aspecten in verband met de informatieveiligheid en de gegevensbescherming.

Teneinde haar opdracht te vervullen dient het Comité Informatie en ICT kennis te nemen van de initiatieven genomen op het vlak van politionele informatie en de ontwikkelingen van systemen. De doelstelling is het onderzoek mogelijk maken van deze initiatieven met het oog op de samenhang van het informatiebeheer of de optimalisatie ervan. Concreet handelt het onder andere over het onderzoek van de projecten of de verzekering van de opvolging ervan.

De inwerkingstelling van een verwerkingsregister binnen de geïntegreerde politie is hiervan een goed voorbeeld. Wat betreft de bijzondere gegevensbanken biedt deze bepaling een antwoord op de aanbevelingen van de onderzoekscommissie belast met het onderzoek naar de omstandigheden die geleid hebben tot de terroristische aanslagen van 22 maart 2016 (deel 3, IV, n° 217). Zonder zich in de plaats te stellen van de verwerkingsverantwoordelijken van deze bijzondere gegevensbanken kan het Comité Informatie en ICT inderdaad kennisnemen van hun bestaan en van hun doelstellingen en kan zij in voorkomend geval, te weten wanneer dit zinvol of noodzakelijk blijkt te zijn, adviezen of aanbevelingen formuleren teneinde de samenhang in het informatiebeheer te garanderen. Het kan bijvoorbeeld aangewezen zijn dat een initiatief van een dienst die een bijzondere gegevensbank heeft ontwikkeld ter beschikking kan gesteld worden van het geheel van diensten door middel van de A.N.G., een basisgegevensbank of koppelingen. Uiteraard zal het in de praktijk niet mogelijk zijn om elk klein genomen initiatief te onderzoeken zodat het bijgevolg toekomt aan het Comité om de beste aanpak van deze opdracht te bepalen.

In haar verslag heeft de voormelde onderzoekscommissie het belang van uitwisseling van informatie (*need to share*) en het onderling verband tussen de verschillende gegevensbanken benadrukt om deze doelstelling te bereiken. De mogelijkheid om aan te leunen bij de expertise van het Comité Informatie en ICT zal ongetwijfeld gunstige gevolgen hebben op het geheel van de politiediensten. In die zin bekrachtigt het officialiseren van het Comité Informatie en ICT de "*gouvernance*" die reeds aanwezig is inzake informatiebeheer.

Het Comité Informatie en ICT is ook bevoegd om adviezen te geven wanneer DPO die ressorteren onder verschillende overheden afwijkende adviezen zouden geven die een impact zouden hebben op de geïntegreerde werking van de politie.

particulier pour les aspects relatifs à la sécurité de l'information et à la protection des données.

Pour accomplir sa mission, le Comité Information et ICT doit pouvoir prendre connaissance d'initiatives prises dans le domaine de l'information policière et de développements de systèmes. L'objectif est de permettre l'examen de ces initiatives dans une perspective de cohérence dans la gestion de l'information ou de l'optimalisation de celle-ci. Concrètement, il s'agit, entre autres, d'examiner des projets ou d'assurer le suivi de ceux-ci.

La mise en œuvre d'un registre des traitements au sein de la police intégrée est un bon exemple en la matière. En ce qui concerne les banques de données particulières, cette disposition apporte une réponse aux recommandations de la commission d'enquête chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 (partie 3, IV, N°217). En effet, sans se substituer aux responsables du traitement de ces banques de données particulières, le Comité information et ICT peut néanmoins prendre connaissance de leur existence et de leurs finalités et formuler, le cas échéant, à savoir lorsque cela a du sens ou parait nécessaire, des avis et recommandations destinés à garantir la cohérence dans la gestion de l'information policière. Il pourrait par exemple être conseillé qu'une initiative d'un service ayant développé une banque de données particulière puisse être mise à la disposition de l'ensemble des services au moyen de la B.N.G., d'une banque de données de base ou d'interconnexions. Bien entendu, il ne sera pas possible en pratique d'examiner chaque petite initiative, de sorte qu'il revient au Comité de déterminer la meilleure approche à adopter pour cette tâche.

Dans son rapport, la commission d'enquête précitée souligne l'importance du partage de l'information (*need to share*) et le lien entre les différentes banques de données pour atteindre ce but. La possibilité de s'appuyer sur l'expertise du Comité Information en ICT aura sans aucun doute des effets positifs pour l'ensemble des services de police. À ce titre, l'officialisation du Comité Information et ICT renforce la gouvernance déjà en place en matière de gestion de l'information.

Le Comité Information et ICT est également compétent pour rendre des avis en cas d'avis divergents de DPO relevant d'autorités différentes qui impacteraient le fonctionnement intégré de la police.

Net zoals geldt voor de andere adviescomités die binnen de geïntegreerde politie werden opgericht (directiecomité, coördinatiecomité), zullen de werkingsmodaliteiten van het Comité Informatie en ICT ter goedkeuring worden voorgelegd aan de ministers van Binnenlandse Zaken en Justitie.

Dergelijk comité functioneert reeds. Er werd gekozen om deze een wettelijk kader te geven, teneinde zijn rol in het beheer van het informatiebeheer, de veiligheid en de bescherming van gegevens te verduidelijken.

Artikelen 29-30 (nieuwe titel)

Het is noodzakelijk om bepaalde nieuwe regelingen op te nemen in de WGP, eerder dan in de WPA, aangezien er hierdoor toepassing van kan gemaakt worden binnen de geïntegreerde politie, ongeacht of het nu gaat over operationele gegevens (titel 2 van de wet gegevensbescherming), dan wel gegevens die vallen onder de toepassing van de AVG.

Teneinde deze artikelen te kunnen bundelen, wordt door het voorgestelde artikel 28 een destijds opgeheven titel hersteld als volgt: “Modaliteiten betreffende de verwerking van persoonsgegevens”.

Om de regelgeving aangaande informatieverwerking te verduidelijken, wordt er door het voorgestelde artikel 29 voorzien in enkele definities, die zullen toelaten verder in de tekst gemakkelijker te verwijzen naar de toepasselijke regelgeving.

Artikel 31 (invoeging artikel 144)

Dit artikel is – in essentie – de herintroductie, in de WGP, van het oude artikel 44/3 van de WPA.

Zoals reeds eerder in deze memorie toegelicht, zullen de taken van veiligheidsconsulent, zoals deze vroeger bestond, in de toekomst verder uitgeoefend worden door de DPO. De bepalingen die vroeger dus van toepassing waren op de veiligheidsconsulent, worden nu – waar nodig – overgeheveld naar de WGP en toegepast op de DPO.

In elk geval heeft elke politiezone minstens een DPO nodig voor het personeelsbestand (AVG) en zal ze er ook één nodig hebben voor eventuele bijzondere gegevensbanken (Titel 2 wet gegevensbescherming). Bijgevolg werd het opportuun geacht om iedereen de verplichting op te leggen om er minstens één aan te stellen die alle opdrachten kan uitvoeren.

Comme pour les autres comités d’avis mis en place au sein de la police intégrée (Comité de direction, Comité de Coordination), les modalités de fonctionnement du Comité Information et ICT seront soumises, pour approbation, aux ministres de l’Intérieur et de la Justice.

Un tel comité fonctionne déjà. Il a été décidé de lui donner un cadre légal afin de clarifier son rôle dans la gouvernance de la gestion de l’information, de la sécurité et de la protection des données.

Articles 29-30 (nouveau titre)

Il est nécessaire d’inclure certaines nouvelles dispositions dans la LPI, plutôt que dans LFP, puisque leur contenu est applicable au sein de la police intégrée, indépendamment du fait qu’il s’agisse de données opérationnelles (titre 2 de la loi relative à la protection des données) ou de données relevant du champ d’application du RGPD.

Afin de pouvoir regrouper ces articles, l’article 28 en proposition réhabilite un titre anciennement abrogé sous l’intitulé: “Modalités relatives au traitement de données à caractère personnel”.

Afin de clarifier la réglementation en matière de traitement de l’information, l’article 29 en proposition prévoit quelques définitions qui permettront de faire plus facilement référence à la réglementation applicable dans la suite du texte.

Article 31 (introduction article 144)

Cet article vise, en substance, à rétablir dans la LPI l’ancien article 44/3 de la LFP.

Comme déjà indiqué dans le début de cet exposé, les tâches du conseiller en sécurité, tel qu’il existait auparavant, seront désormais exercées par le DPO. Les dispositions qui s’appliquaient précédemment au conseiller en sécurité sont désormais, là où c’est nécessaire, transférées dans la LPI et appliquées au DPO.

En tous cas, chaque zone de police a besoin d’au moins un DPO pour le fichier du personnel (RGPD) et en aura également besoin d’un pour les éventuelles banques de données particulières (Titre 2 de la loi relative à la protection des données). Il a dès lors paru opportun d’imposer à tout le monde l’obligation d’en désigner au moins un qui peut effectuer l’ensemble des missions.

Net zoals de met de verplichting bepaald in artikel 21 van de wet gegevensbescherming om de aanwijzing van een DPO binnen de bedrijven die een verwerking uitvoeren voor de verwerkingsverantwoordelijke te eisen, vereist artikel 144 van alle verwerkers van politiediensten en van alle autoriteiten die toegang hebben tot het communicatiesysteem of tot verwerkingen van gegevens van politiediensten, dat zij een DPO aan wijzen. Dit heeft ook betrekking op de autoriteiten bedoeld in artikel 44/11/7, 44/11/8 en 44/11/9, wanneer zij een link hebben met het informatiesysteem van de politiediensten. Dit heeft ook betrekking op NV ASTRID die als verwerker de informatiesystemen van het Informatie- en Communicatiecentrum en van de politiescholen beheert. De verplichting om lid te zijn van de politiediensten is niet van toepassing op deze DPO's.

Hypothetisch gezien bestaat uiteraard de mogelijkheid dat er geen bijzondere gegevensbanken of geen verwerkingen AVG zijn, dan nog zijn er andere taken mogelijk voor een DPO, die desgevallend omschreven zullen worden in een KB.

De mogelijkheid voor dergelijke bijkomende taken wordt geregeld in artikel 38.6 van de AVG en artikelen 63, vijfde lid, en 64, zesde lid, van de wet gegevensbescherming.

De Koning wordt belast met het nader bepalen van de missies en de werkwijzen van de DPO's. Dit KB zal het KB van 6 december 2015 betreffende de consulenten voor de veiligheid en de bescherming van de persoonlijke levenssfeer vervangen.

De nadere regels uiteengezet in dit koninklijk besluit zijn uitsluitend van toepassing op DPO's die binnen de politiediensten zijn aangewezen.

Artikel 32 (invoeging artikel 145)

Het verwerkingsregister wordt ontwikkeld in die zin om ook in een communicatiekanaal te voorzien met het Controleorgaan. Zowel in zijn advies nr. 009/2018 van 12 december 2018, alsook in advies 65.312/2 van de Raad van State van 4 maart 2019 is de introductie van een uniek communicatiemiddel tussen het Controleorgaan en het politiewezen ondersteund.

Eveneens met als doel een geïntegreerde werking van de politiediensten mogelijk te maken, wordt in dit artikel bepaald dat de Koning de nadere regels zal bepalen voor de vorm, de inhoud en de beheersmodaliteiten van het verwerkingsregister van de geïntegreerde

À l'instar de l'obligation prévue à l'article 21 de la loi relative à la protection des données d'exiger la désignation d'un DPO au sein des sociétés qui effectuent une sous-traitance pour le responsable de traitement, l'article 144 requiert de tous les sous-traitants des services de police et de toutes les autorités ayant un accès au système de communication ou aux traitements de données des services de police de désigner un délégué à la protection des données. Sont ainsi visées les autorités visées à l'article 44/11/7, 44/11/8 et 44/11/9 si elles disposent d'une connexion au système d'information des services de police. Sont également visées, la SA ASTRID comme sous-traitant gérant les systèmes d'information des Centre d'information et de Communication et les académies de police. L'obligation d'être membre des services de police ne s'applique pas à ces DPO.

Hypothétiquement, il est évidemment possible de ne pas avoir de banques de données particulières ni de traitements RGPD, mais dans pareil cas, le DPO peut avoir d'autres tâches, qui seront le cas échéant décrites par AR.

La possibilité d'avoir de telles tâches supplémentaires est prévue à l'article 38.6 du RGPD et aux articles 63, alinéa 5, et 64, alinéa 6, de la loi relative à la protection des données.

Le Roi est chargé de préciser les missions et les modalités de fonctionnement des DPO. Cet AR remplacera l'AR du 06 décembre 2015 relatif aux conseillers en sécurité et en protection de la vie privée.

Les modalités prévues dans cet arrêté royal s'appliquent exclusivement aux DPO désignés au sein des services de police.

Article 32 (introduction article 145)

Le registre des activités de traitement est élaboré de manière à constituer également un canal de communication privilégié avec l'Organe de contrôle. Tant ce dernier, dans son avis n° 009/2018 du 12 décembre 2018, que le Conseil d'État, dans son avis 65.312/2 du 4 mars 2019 ont soutenu l'introduction d'un outil de communication standard et unique entre l'Organe de contrôle et l'ensemble de la police intégrée.

Dans le but de permettre un fonctionnement intégré des services de police, cet article prévoit que le Roi fixe des règles plus précises quant à la forme, au contenu et aux modalités de gestion du registre des activités de traitement, tant pour ce qui concerne les traitements

politie, zowel voor wat betreft de verwerkingen die onder het toepassingsgebied van de AVG vallen, als deze die vallen onder de wet gegevensbescherming. Alle verwerkingen die worden uitgevoerd door de politiezones en de federale politie, ongeacht de verwerkingsverantwoordelijk, worden daar geregistreerd.

Artikel 33 (invoeging artikel 146)

Hoewel artikel 5 van de AVG bepaalt dat een verdere verwerking van de persoonsgegevens toegestaan is voor zover de doeleinden niet onverenigbaar zijn, zou de verwerkingsverantwoordelijke kunnen beslissen om ze niet aan een andere verwerkingsverantwoordelijke mee te delen.

Artikel 1, 3°, AVG bepaalt dat "het vrije verkeer van persoonsgegevens in de Unie wordt noch beperkt noch verboden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens", is om iedere blokkering binnen de geïntegreerde politie te vermijden en alle verwerkingsverantwoordelijken in staat te stellen hun opdrachten uit te voeren, waaronder het personeelsbeheer zoals bepaald op grond van het statuut, bepaalt artikel 146 dat ze de persoonsgegevens die onder het toepassingsgebied van de AVG vallen, aan elkaar meedelen.

Het gaat om de uitwisselingen tussen politiezones, tussen politiezones en de Federale Politie of met bijvoorbeeld de politiescholen, het sociaal secretariaat van de geïntegreerde politie (SSGPI) of de sociale dienst (SSDGPI). De twee laatstgenoemde entiteiten kunnen verwerker en verwerkingsverantwoordelijke zijn, naargelang van de opdrachten waarmee ze worden belast. Deze gegevensuitwisselingen blijven uiteraard onderworpen aan de algemene beginselen van proportionaliteit en noodzaak zoals bepaald in artikel 5 van de AVG.

TITEL III

Overgangs-, opheffings- en slotbepalingen

Artikel 34

De uitvoering van de bepalingen van de wet gegevensbescherming op het vlak van logging vormt een uitdaging.

De informaticasystemen van de politiediensten worden gemoderniseerd. Er worden grote inspanningen geleverd opdat deze verplichting om logbestanden te verwerken zoals bepaald in artikel 56 van de wet

tombant sous le champ d'application du RGPD que ceux qui relèvent de la loi relative à la protection des données. Tous les traitements effectués par les zones de police et la police fédérale, et ce quel que soit le responsable du traitement, y seront enregistrés.

Article 33 (introduction article 146)

Bien que l'article 5 du RGPD prévoit qu'un traitement ultérieur des données à caractère personnel est autorisé pour autant que les finalités ne soient pas incompatibles, le responsable de traitement pourrait décider de ne pas les communiquer à un autre responsable de traitement.

L'article 1er, 3°, du RGPD prévoit 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". Afin d'éviter tout blocage au sein de la police intégrée et permettre à l'ensemble des responsables de traitement d'exécuter leurs missions, dont la gestion du personnel, comme prévu en application du statut, l'article 146 dispose qu'ils se communiquent les données à caractère personnel qui relèvent du champ d'application du RGPD.

Sont entre autres visés les échanges entre zones de police, entre zones de police et la Police Fédérale ou avec, par exemple, les académies de police, le secrétariat social de la police intégrée (SSGPI) ou le service social (SSDGPI). Ces dernières entités pouvant agir en tant que sous-traitants et responsables de traitement en fonction des missions dont elles sont chargées. Ces échanges de données restent évidemment soumis aux principes généraux de proportionnalité et de nécessité tels que visés à l'article 5 du RGPD.

TITRE III

Dispositions transitoires, abrogatoires et finales

Article 34

La mise en œuvre des dispositions de la loi relative à la protection des données en matière de journalisation constitue un défi.

Les systèmes informatiques des services de police sont en cours de modernisation. Des efforts substantiels sont mis en œuvre afin que cette obligation de traiter des fichiers de journalisation, prévue à l'article 56 de la

gegevensbescherming (tot omzetting van artikel 25 van de Richtlijn), zo snel mogelijk kan worden verwezenlijkt voor alle geautomatiseerde verwerkingssystemen die vóór 6 mei 2016 werden geïnstalleerd. Deze moeilijkheid is het Parlement en de Europese Raad niet ontgaan.

Bijgevolg, terwijl de artikelen 10, 4°, 11 en 13, 3°, en artikel 14, 3°, tweede lid, het principe en de modaliteiten van deze verplichting vastleggen, laat artikel 34, in overeenstemming met artikel 279 van de wet gegevensbescherming, de politiediensten toe om de geautomatiseerde verwerkingssystemen die geïnstalleerd werden vóór 6 mei 2016 in overeenstemming te brengen, wanneer voor deze overeenstemming bovenmatige inspanningen nodig zijn, ten laatste op 6 mei 2023.

Zo hebben de politiediensten de mogelijkheid om zich geleidelijk aan te passen om de geplande doelstelling te bereiken rekening houdend met de technische en budgettaire gevolgen die deze nieuwe verplichtingen met zich meebrengen.

Franky DEMON (CD&V)
Veerle HEEREN (CD&V)
Katja GABRIËLS (Open Vld)
Sandrine DE CROM (Open Vld)

loi relative à la protection des données (qui transpose l'article 25 de la Directive) puisse être au plus vite effective pour tous les systèmes de traitement automatisés installés avant le 6 mai 2016. Cette difficulté n'a pas échappé au Parlement et au Conseil européens.

Par conséquent, si les articles 10, 4°, 11 et 13, 3°, ainsi que l'article 14, 3°, al. 2 consacrent le principe et les modalités de cette obligation, l'article 34, conformément à l'article 279 de la loi relative à la protection des données, permet aux services de police de mettre en conformité les systèmes de traitement automatisés installés avant le 6 mai 2016, lorsque cette mise en conformité exige des efforts disproportionnés, au plus tard le 6 mai 2023.

La possibilité est ainsi laissée aux services de police de s'adapter progressivement pour atteindre l'objectif prévu compte tenu des impacts techniques et budgétaires qu'engendrent ces nouvelles obligations.

WETSVOORSTEL

TITEL I

Algemene bepaling

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

TITEL II

Wijzigingsbepalingen

HOOFDSTUK I

Wijzigingen van de wet op het politieambt

Art. 2

In artikel 3 van de wet op het politieambt, gewijzigd bij de wet van 19 juli 2018, worden de volgende wijzigingen aangebracht:

1° onder 6° worden de woorden “artikel 36*ter* van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van de persoonsgegevens” vervangen door de woorden “artikel 71 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens”;

2° het artikel wordt aangevuld met een bepaling onder 10°, luidende:

“10° wet gegevensbescherming: de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.”.

Art. 3

In artikel 25/8 van dezelfde wet, ingevoegd bij de wet van 21 maart 2018, wordt het derde lid vervangen als volgt:

“De in het eerste en tweede lid bedoelde registers worden, op verzoek, ter beschikking gesteld van het Controleorgaan, van de bestuurlijke en gerechtelijke politieoverheden en van de functionaris voor

PROPOSITION DE LOI

TITRE I^ER

Disposition générale

Article 1er

La présente loi règle une matière visée à l’article 74 de la Constitution.

TITRE II

Dispositions modificatives

CHAPITRE I^ER

Modifications de la loi sur la fonction de police

Art. 2

À l’article 3 de la loi sur la fonction de police, modifié par la loi du 19 juillet 2018, les modifications suivantes sont apportées:

1° au 6°, les mots “article 36*ter* 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” sont remplacés par les mots “article 71 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l’égard du traitement de données à caractère personnel”;

2° l’article est complété par un 10°, rédigé comme suit:

“10° loi relative à la protection des données: la loi du 30 juillet 2018 relative à la protection des personnes physiques à l’égard du traitement de données à caractère personnel.”.

Art. 3

À l’article 25/8 de la même loi, inséré par la loi du 21 mars 2018, l’alinéa 3 est remplacé comme suit:

“Les registres visés aux alinéas 1er et 2 sont mis à la disposition, sur demande, de l’Organe de contrôle, des autorités de police administrative et judiciaire et du délégué à la protection des données visé à l’article 144

gegevensbescherming bedoeld in artikel 144 van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus.”.

Art. 4

In artikel 44/1 van dezelfde wet, ingevoegd bij de wet van 18 maart 2014 en gewijzigd bij de wet van 21 maart 2018, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 worden de woorden “en overeenkomstig de doeleinden omschreven in artikel 27 van de wet gegevensbescherming” ingevoegd tussen de woorden “afdeling 1,” en “kunnen”;

2° paragraaf 2 wordt vervangen als volgt:

“§ 2. Met het oog op het uitoefenen van hun opdrachten mogen de politiediensten de persoonsgegevens zoals bedoeld in artikel 34 van de wet gegevensbescherming verwerken ter aanvulling of ondersteuning van de andere categorieën van gegevens zoals bedoeld in artikel 44/5.

Naast de voorwaarde bedoeld in het eerste lid geldt het volgende:

1° de biometrische gegevens worden enkel verwerkt met het oog op het verzekeren van de ondubbelzinnige identificatie van de betrokken persoon;

2° de gegevens betreffende gezondheid worden enkel verwerkt 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;

3° de verwerking van genetische gegevens betreft enkel het inwinnen van genetische gegevens en de registratie van administratieve vermeldingen verbonden aan het genetisch profiel, met uitsluiting van de vergelijking van genetische profielen of de identificatie van het DNA-codenummer en wordt uitgevoerd in het kader van de uitoefening van opdrachten van gerechtelijke politie en de toepassing van de wetgeving inzake civiele bescherming.

Tijdens de in deze paragraaf bedoelde verwerkingen van persoonsgegevens zijn de volgende waarborgen inzake bescherming van persoonsgegevens van toepassing:

de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux.”.

Art. 4

À l’article 44/1 de la même loi, inséré par la loi du 18 mars 2014 et modifié par la loi du 21 mars 2018, les modifications suivantes sont apportées:

1° au paragraphe 1er, les mots “et conformément aux finalités fixées à l’article 27 de la loi relative à la protection des données” sont insérés entre les mots “section 1re,” et “les services”;

2° le paragraphe 2 est remplacé comme suit:

“§ 2. En vue d’exercer leurs missions, les services de police peuvent traiter les catégories particulières de données à caractère personnel visées à l’article 34 de la loi relative à la protection des données en complément ou en soutien d’autres catégories de données visées à l’article 44/5.

En plus de la condition visée à l’alinéa 1er:

1° les données biométriques sont traitées uniquement dans le but d’assurer l’identification certaine de la personne concernée;

2° les données relatives à la santé sont traitées 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;

3° le traitement des données génétiques concerne uniquement la collecte des données génétiques et l’enregistrement des mentions administratives liées au profil génétique, à l’exclusion de la comparaison des profils génétiques ou de l’identification du numéro de code ADN et s’effectue dans le cadre de l’exercice des missions de police judiciaire et de l’application de la législation relative à la protection civile.

Lors des traitements de données à caractère personnel visées dans ce paragraphe, les garanties suivantes en matière de protection des données à caractère personnel sont d’application:

1° de categorieën personen die toegang hebben tot de persoonsgegevens worden aangewezen door de verwerkingsverantwoordelijke of, in voorkomend geval, door de verwerker, met een beschrijving van hun functie ten aanzien van de verwerking van de gegevens in kwestie;

2° de lijst van de aangewezen personen om de in deze paragraaf bedoelde gegevens te verwerken, stelt de verwerkingsverantwoordelijke of, in voorkomend geval, de verwerker ter beschikking van het Controleorgaan;

3° de aangewezen personen moeten, op grond van een wettelijke of statutaire verplichting, of een overeenkomstige contractuele bepaling, het vertrouwelijke karakter van de gegevens in kwestie in acht nemen;

4° er wordt een duidelijk onderscheid gemaakt tussen de in artikel 44/5 bedoelde categorieën van personen;

5° er worden gepaste technische of organisatorische maatregelen getroffen om de persoonsgegevens tegen toevallige of niet-toegelaten vernietiging, tegen toevallig verlies of elke andere niet-toegelaten verwerking van die gegevens te beschermen;

6° de verwerkingsverantwoordelijken vermelden in hun gegevensbeschermingsbeleid de te ondernemen acties om de verwerking van die gegevenscategorieën te beschermen. De bevoegde functionarissen voor gegevensbescherming zien erop toe dat dat beleid gevolgd wordt.

De koning kan in andere gepaste aanvullende waarborgen voorzien.”.

Art. 5

In hoofdstuk IV, afdeling 12 van dezelfde wet, ingevoegd bij de wet van 18 maart 2014 en gewijzigd bij de wet van 21 maart 2018, worden de woorden “Onderafdeling 2 – De consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer” opgeheven.

Art. 6

In artikel 44/3 van dezelfde wet, ingevoegd bij de wet van 18 maart 2014, gewijzigd bij de wetten van 26 maart 2014, 27 april 2016 en 21 maart 2018, worden de volgende wijzigingen aangebracht:

1° les catégories de personnes, ayant accès aux données à caractère personnel, sont désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description de leur fonction par rapport au traitement des données visées;

2° la liste des catégories des personnes ainsi désignées pour traiter les données visées dans ce paragraphe est tenue à la disposition de l’Organe de contrôle par le responsable du traitement ou, le cas échéant, par le sous-traitant;

3° les personnes désignées sont tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées;

4° une distinction claire est opérée entre les catégories de personnes visées à l’article 44/5;

5° des mesures techniques ou organisationnelles appropriées sont adoptées 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;

6° les responsables du traitement indiquent dans leur politique de protection des données les actions à mener pour protéger le traitement de ces catégories de données. Les délégués à la protection des données compétents veillent à assurer le suivi de cette politique.

Le Roi peut prévoir d’autres garanties complémentaires appropriées.”.

Art. 5

Au chapitre IV, section 12 de la même loi, inséré par la loi du 18 mars 2014 et modifié par la loi du 21 mars 2018, les mots “Sous-section 2 – Le conseiller en sécurité et en protection de la vie privée” sont abrogés.

Art. 6

À l’article 44/3 de la même loi, inséré par la loi du 18 mars 2014 et modifié par les lois du 26 mars 2014, du 27 avril 2016 et du 21 mars 2018, les modifications suivantes sont apportées:

1° in paragraaf 1 worden de woorden “de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens” vervangen door de woorden “de wet gegevensbescherming”;

2° in paragraaf 1 worden het derde tot en met het achtste lid opgeheven;

3° paragrafen 1/1 en 2 worden opgeheven.

Art. 7

Artikel 44/4 van dezelfde wet, ingevoegd bij de wet van 18 maart 2014, gewijzigd bij de wetten van 26 maart 2014, 27 april 2016 en 21 maart 2018, wordt vervangen als volgt:

“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

1° au paragraphe 1er, les mots “la loi du 8 décembre 1992 relative à la protection de la vie privée à l’égard des traitements de données à caractère personnel” sont remplacés par les mots “la loi relative à la protection des données”;

2° au paragraphe 1er, les alinéas 3 à 8 sont abrogés;

3° les paragraphes 1er/1 et 2 sont abrogés.

Art. 7

L’article 44/4 de la même loi, inséré par la loi du 18 mars 2014, modifié par les lois du 26 mars 2014, du 27 avril 2016 et du 21 mars 2018 est remplacé comme suit:

“Art. 44/4 § 1er. 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, § 1er, 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, § 1er, 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,

wijziging, de raadpleging, de mededeling, met inbegrip van de doorgiften, de archivering, de koppeling en de uitwissing.

De log-, raadplegings- en mededelingsbestanden 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 in de Ministerraad overlegd besluit, 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 Justitie, elk binnen het kader van hun bevoegdheden, bij richtlijn, de toegangsregels

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° et 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 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, § 1er, 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 les règles d'accès des membres

voor de leden van de politiediensten tot de gegevensbanken bedoeld in artikel 44/2, § 1 en § 3.

§ 3*bis*. De Ministers van Binnenlandse Zaken en Justitie bepalen, elk binnen het kader van hun bevoegdheden, bij richtlijn de modaliteiten 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 modaliteiten betreffende de koppeling en de toegangsregels van de leden van de politiediensten tot de daaruit voortvloeiende verwerkingen.

§ 3*ter*. De in de paragrafen 3 en 3*bis* bedoelde profielen en toegangsmodaliteiten 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 in artikel 44/5 bedoelde personen;

4° van de evaluatie van de gegevens;

5° van de validatiestatus van de verwerkte gegevens.

De in de paragrafen 3 en 3*bis* 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.

§ 4. De ministers van Binnenlandse Zaken en van Justitie bepalen bij gemeenschappelijke richtlijn 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.

des services de police aux banques de données visées à l'article 44/2, § 1er, et § 3.

§ 3*bis*. Les ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences, déterminent par directive 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 aux traitements qui en résultent.

§ 3*ter*. Les profils et les modalités d'accès visés aux paragraphes 3 et 3*bis* 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 paragraphes 3 et 3*bis* 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.

§ 4. Les ministres de l'Intérieur et de la Justice déterminent par directives communes 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.

Deze gemeenschappelijke 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.”.

Art. 8

In artikel 44/5 van dezelfde wet, ingevoegd bij de wet van 18 maart 2014 en gewijzigd bij de wet van 27 april 2016, worden de volgende wijzigingen aangebracht:

1° het eerste lid van paragraaf 1 wordt aangevuld met een 7°, luidende:

“7° de gegevens betreffende personen die het voorwerp uitmaken van een bestuurlijke maatregel genomen door een bevoegde bestuurlijke overheid en dewelke de politiediensten krachtens de wet, het decreet of de ordonnantie gelast zijn deze op te volgen.”;

2° paragraaf 3, 8°, wordt vervangen als volgt:

“8° de gegevens met betrekking tot de personen bedoeld in de artikelen 47*novies*/1, § 1, 47*decies*, § 1, en 102, 1° tot 3°, van het Wetboek van strafvordering;”;

3° in paragraaf 6 worden de woorden “niet langer juist zijn of” ingevoegd tussen de woorden “de gegevens” en “niet langer beantwoorden”;

4° een paragraaf 7 wordt ingevoegd, luidende:

“§ 7. In specifieke omstandigheden kunnen de gegevens bedoeld in § 4 daarenboven verwerkt worden in de gegevensbank bedoeld in artikel 44/2, § 1, 1°.”.

Art. 9

In hoofdstuk IV, afdeling 12 van dezelfde wet, ingevoegd bij de wet van 18 maart 2014 en gewijzigd bij de wet van 21 maart 2018, wordt onderafdeling 4, bestaande uit artikel 44/6, opgeheven.

Art. 10

In artikel 44/9 van dezelfde wet, ingevoegd bij de wet van 18 maart 2014 en gewijzigd bij de wet van 31 oktober 2017, worden de volgende wijzigingen aangebracht:

Ces directives communes tiennent 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.”.

Art. 8

À l’article 44/5 de la même loi, inséré par la loi du 18 mars 2014 et modifié par la loi du 27 avril 2016, les modifications suivantes sont apportées:

1° l’alinéa 1er du paragraphe 1er est complété par un 7° rédigé comme suit:

“7° les données relatives aux personnes faisant l’objet d’une mesure administrative prise par une autorité administrative compétente et que les services de police sont chargés de suivre par ou en vertu de la loi, du décret ou de l’ordonnance.”;

2° le paragraphe 3, 8°, est remplacé comme suit:

“8° les données relatives aux personnes visées aux articles 47*novies*/1, § 1er, 47*decies*, § 1er, et 102, 1° à 3°, du Code d’instruction criminelle;”;

3° au paragraphe 6, les mots “ne sont plus exactes ou” sont insérés entre les mots “les données” et “ne remplissent plus”;

4° il est inséré un paragraphe 7, rédigé comme suit:

“§ 7. Dans des circonstances spécifiques, les données visées au § 4 peuvent en outre être traitées dans la banque de données visée à l’article 44/2, § 1er, 1°.”.

Art. 9

Dans le chapitre IV, section 12 de la même loi, inséré par la loi du 18 mars 2014 et modifié par la loi du 21 mars 2018, la sous-section 4, comprenant l’article 44/6, est abrogée.

Art. 10

À l’article 44/9 de la même loi, inséré par la loi du 18 mars 2014 et modifié par la loi du 31 octobre 2017, les modifications suivantes sont apportées:

1° in paragraaf 1, eerste lid, 1°, worden de woorden “artikel 44/5, § 1, 1°” vervangen door de woorden “artikel 44/5, § 1, 1° en 7°”;

2° in paragraaf 1, tweede lid, worden de woorden “2° tot 6°” vervangen door de woorden “2° tot 7°”;

3° in paragraaf 2, a),worden de woorden “en § 4, 2°” ingevoegd tussen de woorden “6°” en “, bedoelde personen”;

4° in paragraaf 2, d), worden de woorden “en § 4, 1°” ingevoegd tussen de woorden “9°” en “, bedoelde personen”;

5° een paragraaf 3 wordt ingevoegd, luidende:

“§ 3. Alle uitgevoerde verwerkingen in de A.N.G. maken het voorwerp uit van logbestanden die bewaard worden gedurende dertig jaar vanaf de in de A.N.G. uitgevoerde verwerking.”.

Art. 11

Artikel 44/10, § 1, van dezelfde wet, ingevoegd bij de wet van 18 maart 2014, wordt aangevuld met een derde lid, luidende:

“Alle uitgevoerde verwerkingen in de archieven van de A.N.G. maken het voorwerp uit van logbestanden die bewaard worden gedurende dertig jaar vanaf de in de archieven van de A.N.G. uitgevoerde verwerking.”.

Art. 12

In artikel 44/11, § 2, van dezelfde wet, ingevoegd bij de wet van 18 maart 2014, worden de woorden “het in artikel 44/6 bedoelde Controleorgaan” vervangen door de woorden “het Controleorgaan”.

Art. 13

In artikel 44/11/2 van dezelfde wet, ingevoegd bij de wet van 18 maart 2014 en gewijzigd bij de wet van 26 maart 2014, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, tweede lid worden de woorden “en beheerd” ingevoegd tussen de woorden “ontwikkeld” en “door”;

2° paragraaf 2 wordt vervangen als volgt:

1° au paragraphe 1er, alinéa 1er, 1°, les mots “l’article 44/5, § 1er, 1°” sont remplacés par les mots “l’article 44/5, § 1er, 1° et 7°”;

2° au paragraphe 1er, alinéa 2, les mots “2° à 6°” sont remplacés par les mots “2° à 7°”;

3° le paragraphe 2, a), est complété par les mots “et § 4, 2°”;

4° au paragraphe 2, d), les mots “et § 4, 1°” sont insérés entre les mots “9°” et “, dix ans”;

5° il est inséré un paragraphe 3, rédigé comme suit:

“§ 3. Tous les traitements réalisés dans la B.N.G. font l’objet d’une journalisation qui est conservée pendant trente ans à partir du traitement réalisé dans la B.N.G.”.

Art. 11

L’article 44/10, § 1er, de la même loi, inséré par la loi du 18 mars 2014, est complété par un alinéa 3, rédigé comme suit:

“Tous les traitements réalisés dans les archives de la B.N.G. font l’objet d’une journalisation qui est conservée pendant trente ans à partir du traitement réalisé dans les archives de la B.N.G.”.

Art. 12

À l’article 44/11, § 2, de la même loi, inséré par la loi du 18 mars 2014, les mots “l’Organe de contrôle visé à l’article 44/6” sont remplacés par les mots “l’Organe de contrôle”.

Art. 13

À l’article 44/11/2 de la même loi, inséré par la loi du 18 mars 2014 et modifié par la loi du 26 mars 2014, les modifications suivantes sont apportées:

1° au paragraphe 1er, alinéa 2, les mots “et gérées” sont insérés entre les mots “développées” et “par”;

2° le paragraphe 2 est remplacé comme suit:

"§ 2. De gegevens die betrekking hebben op de opdrachten van bestuurlijke politie zijn toegankelijk gedurende vijf jaar vanaf de dag van de registratie ervan.

De gegevens die betrekking hebben op de opdrachten van gerechtelijke politie zijn toegankelijk gedurende vijftien jaar vanaf de dag van de registratie ervan.";

3° in de paragrafen 3, 4 en 5, worden de woorden "in § 2, derde lid" vervangen door de woorden "in § 2, tweede lid";

4° een paragraaf 8 wordt ingevoegd, luidende:

"§ 8. Alle uitgevoerde verwerkingen in de basisgegevensbanken maken het voorwerp uit van logbestanden die bewaard worden gedurende vijftien jaar vanaf de in de basisgegevensbanken uitgevoerde verwerking. De verwerkingsverantwoordelijke kan, indien nodig, deze termijn verlengen met een maximale periode van vijftien jaar.".

Art. 14

In artikel 44/11/3 van dezelfde wet, ingevoegd bij de wet van 18 maart 2014 en gewijzigd bij de wetten van 26 maart 2014 en 27 april 2016, worden de volgende wijzigingen aangebracht:

1° paragraaf 1 wordt vervangen als volgt:

"§ 1. In specifieke omstandigheden kunnen de korpschefs, de commissaris-generaal, de directeurs-generaal en de directeurs, voor bijzondere behoeften, bijzondere gegevensbanken oprichten waarvoor ze verwerkingsverantwoordelijke zijn, teneinde de erin vervatte gegevens verder te verwerken in het kader van de uitoefening van hun opdrachten en doeleinden van bestuurlijke en gerechtelijke politie.

De categorieën van gegevens bedoeld in artikel 44/5 mogen eveneens verwerkt worden in de bijzondere gegevensbanken voor zover de verwerking toereikend, terzake dienend en niet overmatig van aard is.";

2° paragraaf 3 wordt vervangen als volgt:

"§ 3. De verwerkingsverantwoordelijke duidt de opdrachten en doeleinden, die de creatie van een bijzondere gegevensbank verantwoorden, aan.

Het Controleorgaan wordt, via het unieke register van de verwerkingsactiviteiten van de politiediensten bedoeld in artikel 145 van de wet van 7 december 1998

"§ 2. Les données relatives aux missions de police administrative sont accessibles durant cinq ans à partir du jour de leur enregistrement.

Les données relatives aux missions de police judiciaire sont accessibles durant quinze ans à partir du jour de leur enregistrement.";

3° dans les paragraphes 3, 4 et 5, les mots "au § 2, alinéa 3" sont remplacés par les mots "au § 2, alinéa 2";

4° il est inséré un paragraphe 8, rédigé comme suit:

"§ 8. Tous les traitements réalisés dans les banques de données de base font l'objet d'une journalisation qui est conservée pendant quinze ans à partir du traitement réalisé dans les banques de données de base. Le responsable du traitement peut, si nécessaire, prolonger ce délai de maximum quinze ans.".

Art. 14

À l'article 44/11/3 de la même loi, inséré par la loi du 18 mars 2014 et modifié par les lois du 26 mars 2014 et du 27 avril 2016, les modifications suivantes sont apportées:

1° le paragraphe 1er est remplacé comme suit:

"§ 1er. Dans des circonstances spécifiques, les chefs de corps, le commissaire général, les directeurs généraux et les directeurs peuvent créer, pour des besoins particuliers, des banques de données particulières dont ils sont responsables du traitement, dans le but de traiter les données qu'elles contiennent dans le cadre de l'exercice de leurs missions et finalités de police administrative et judiciaire.

Les catégories de données visées à l'article 44/5 peuvent également être traitées dans des banques de données particulières pour autant que ce traitement soit adéquat, pertinent et non excessif.";

2° le paragraphe 3 est remplacé comme suit:

"§ 3. Le responsable du traitement rend compte des missions et finalités qui justifient la création d'une banque de données particulière.

L'Organe de contrôle est averti activement, via le registre unique des activités de traitement des services de police visé à l'article 145 de la loi du 7 décembre 1998

tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, actief op de hoogte gebracht van de aanmaak of van wijzigingen in dat register met betrekking tot een bijzondere gegevensbank.";

3° paragraaf 4 wordt vervangen als volgt:

"§ 4. Onverminderd de registratie of de archivering van de gegevens in overeenstemming met de artikelen 44/2, § 1, tweede lid, 1°, en 44/10, worden deze gegevens en de bijzondere gegevensbanken gewist van zodra de in § 1 bedoelde bijzondere behoeften verdwijnen.

De logbestanden van de verwerkingen worden bewaard gedurende minimum tien jaar. De verwerkingsverantwoordelijke kan, indien nodig, bij een gemotiveerde beslissing en na evaluatie deze termijn verlengen met een maximale periode van twintig jaar.";

4° paragraaf 5 wordt opgeheven.

Art. 15

In artikel 44/11/3*bis* van dezelfde wet, ingevoegd bij de wet van 27 april 2016, worden de volgende wijzigingen aangebracht:

1° in paragraaf 3 worden de woorden "het Orgaan bedoeld in artikel 44/6, tweede lid" vervangen door de woorden "het Controleorgaan bedoeld in artikel 44/11/3*quinquies*/2";

2° in paragraaf 4, tweede lid, en in paragraaf 8 worden de woorden "de Commissie voor de bescherming van de persoonlijke levenssfeer" vervangen door "het Comité en het Controleorgaan bedoeld in artikel 44/11/3*quinquies*/2";

3° in paragraaf 9, tweede lid, 5e streepje; worden de woorden "de consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer" vervangen door de woorden "de functionaris voor gegevensbescherming bedoeld in artikel 44/11/3*quinquies*/1".

Art. 16

In artikel 44/11/3*ter* van dezelfde wet, ingevoegd bij de wet van 27 april 2016, worden de volgende wijzigingen aangebracht:

1° paragraaf 1 wordt aangevuld met een lid, luidende:

organisant un service de police intégré, structuré à deux niveaux, de la création ou de modifications dans ce registre relatives à une banque de données particulière.";

3° le paragraphe 4 est remplacé comme suit:

"§ 4. Sans préjudice de l'enregistrement ou de l'archivage des données conformément aux articles 44/2, § 1er, alinéa 2, 1°, et 44/10, ces données et les banques de données particulières sont supprimées dès que les besoins particuliers visés au § 1er disparaissent.

La journalisation des traitements est conservée pendant au minimum dix ans. Le responsable du traitement peut, si nécessaire, après évaluation et de manière motivée, prolonger ce délai de maximum vingt ans.";

4° le paragraphe 5 est abrogé.

Art. 15

À l'article 44/11/3*bis* de la même loi, inséré par la loi du 27 avril 2016, les modifications suivantes sont apportées:

1° au paragraphe 3, les mots "Organe visés à l'article 44/6, alinéa 2" sont remplacés par les mots "l'Organe de contrôle visés à l'article 44/11/3*quinquies*/2";

2° au paragraphe 4, alinéa 2, et au paragraphe 8, les mots "de la Commission de la protection de la vie privée" sont remplacés par les mots "du Comité et de l'Organe de contrôle visés à l'article 44/11/3*quinquies*/2";

3° au paragraphe 9, alinéa 2, 5ème tiret, les mots "du conseiller en sécurité et en protection de la vie privée" sont remplacés par les mots "du délégué à la protection des données visé à l'article 44/11/3*quinquies*/1".

Art. 16

À l'article 44/11/3*ter* de la même loi, inséré par la loi du 27 avril 2016, les modifications suivantes sont apportées:

1° le paragraphe 1er est complété par un alinéa, rédigé comme suit:

"In het kader van de uitoefening van hun opdrachten bedoeld in artikel 44/11/3*quinquies*/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 44/11/3*quinquies*/2.";

2° in de paragrafen 2 en 3 worden de woorden "de Commissie voor de bescherming van de persoonlijke levenssfeer" vervangen door "het Comité en het Controleorgaan bedoeld in artikel 44/11/3*quinquies*/2".

Art. 17

In hoofdstuk IV, afdeling 12, onderafdeling 7*bis* van dezelfde wet, ingevoegd bij de wet 27 april 2016, wordt een artikel 44/11/3*quinquies*/1 ingevoegd, luidende:

"Art. 44/11/3*quinquies*/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.

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 Koning of die hem door de ministers van Binnenlandse Zaken en Justitie worden toevertrouwd.

Hij oefent zijn functie uit, volledig onafhankelijk van de overheden, organen, instellingen, diensten en directies bedoeld in artikel 44/11/3*ter*. Hij brengt rechtstreeks verslag uit bij de ministers van Binnenlandse Zaken en Justitie.".

"Dans le cadre de l'exercice de leurs missions visées à l'article 44/11/3*quinquies*/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 44/11/3*quinquies*/2.";

2° dans les paragraphes 2 et 3, les mots "de la Commission de la protection de la vie privée" sont remplacés par les mots "du Comité et de l'Organe de contrôle visés à l'article 44/11/3*quinquies*/2".

Art. 17

Dans le chapitre IV, section 12, sous-section 7*bis* de la même loi, insérée par la loi du 27 avril 2016, il est inséré un article 44/11/3*quinquies*/1, rédigé comme suit:

"Art. 44/11/3*quinquies*/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 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.

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. 18

In dezelfde onderafdeling 7*bis* van dezelfde wet, ingevoegd bij de wet van 27 april 2016, wordt een artikel 44/11/3*quinquies*/2 ingevoegd, luidende:

"Art. 44/11/3*quinquies*/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:

a) het Controleorgaan;

b) 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. 19

In artikel 44/11/3*septies*, 2°, van dezelfde wet, ingevoegd bij de wet van 21 maart 2018, worden de woorden "2° tot 5°" vervangen door de woorden "2° tot 5° en 7°".

Art. 20

In artikel 44/11/8 van dezelfde wet, ingevoegd bij de wet van 18 maart 2014 en gewijzigd bij de wet van 19 juli 2018, worden de woorden "en aan het Coördinatieorgaan voor de dreigingsanalyse" geschrapt.

Art. 21

Er wordt een artikel 44/11/8*bis* ingevoegd, luidende:

"Art. 44/11/8*bis*. Overeenkomstig de modaliteiten vastgelegd in de richtlijnen van de ministers van Binnenlandse Zaken en Justitie, elk in het kader van hun bevoegdheden, kunnen de persoonsgegevens en de informatie ook worden meegedeeld aan het Coördinatieorgaan voor de dreigingsanalyse en aan de veiligheidsdiensten, onverminderd artikel 14 van de organieke wet van 30 november 1998 betreffende de inlichtingen- en veiligheidsdiensten, om hen toe te laten hun wettelijke opdrachten uit te oefenen.

Art. 18

Dans la même sous-section 7*bis* de la même loi, insérée par la loi du 27 avril 2016, il est inséré un article 44/11/3*quinquies*/2, rédigé comme suit:

"Art. 44/11/3*quinquies*/2. Dans le respect de l'exercice de leurs missions respectives, le contrôle du 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:

a) l'Organe de contrôle;

b) le Comité permanent de contrôle des services de renseignement et de sécurité, visé à l'article 28 de 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.

Ils peuvent à tout moment émettre les recommandations qu'ils estiment nécessaires pour les traitements réalisés dans les banques de données communes.".

Art. 19

À l'article 44/11/3*septies*, 2°, de la même loi, inséré par la loi du 21 mars 2018, les mots "2° à 5°" sont remplacés par les mots "2° à 5° et 7°".

Art. 20

À l'article 44/11/8 de la même loi, inséré par la loi du 18 mars 2014 et modifié par la loi du 19 juillet 2018, les mots "et à l'Organe pour la coordination de l'analyse de la menace" sont supprimés.

Art. 21

Il est inséré un article 44/11/8*bis*, rédigé comme suit:

"Art. 44/11/8*bis*. Selon les modalités déterminées par les directives des ministres de l'Intérieur et de la Justice, chacun dans le cadre de ses compétences, les données à caractère personnel et les informations peuvent aussi être communiquées à l'Organe pour la coordination de l'analyse de la menace et aux services de renseignement et de sécurité, sans préjudice de l'article 14 de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, pour leur permettre d'exercer leurs missions légales.

De modaliteiten voor mededeling aan de politie van de gegevens van de veiligheidsdiensten zijn bepaald in een juridisch instrument waarvan de datum van inwerkingtreding simultaan is aan die van de rechtstreekse toegang van de inlichtingen en veiligheidsdiensten tot de A.N.G.”.

Art. 22

In artikel 44/11/9 van dezelfde wet, ingevoegd bij de wet van 18 maart 2014, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 worden de bepalingen onder 1° tot 4°, vervangen als volgt:

“1° de Cel voor financiële informatieverwerking;

2° de Dienst vreemdelingenzaken;

3° de onderzoeks- en opsporingsdiensten en de administratie toezicht, controle en vaststellingen van de Algemene Administratie der douane en accijnzen.”;

2° paragraaf 2 wordt vervangen als volgt:

“§ 2. Overeenkomstig de modaliteiten vastgelegd in de richtlijnen van de ministers van Binnenlandse Zaken en Justitie, elk in het kader van hun bevoegdheden, kunnen ze eveneens meegedeeld worden aan de Belgische openbare overheden, publieke organen of instellingen of instellingen van openbaar nut die door de wet belast zijn met de toepassing van de strafwet of die wettelijke verplichtingen inzake de openbare veiligheid hebben, wanneer deze ze nodig hebben voor de uitoefening van hun wettelijke opdrachten.

De lijst van deze overheden, organen of instellingen wordt vastgesteld door de ministers van Binnenlandse Zaken en Justitie op basis van een voorstel van het Comité Informatie en ICT bedoeld in artikel 8*sexies* van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus.”.

3° in paragraaf 3 worden de woorden “commissaris-generaal van de federale politie” vervangen door het woord “verwerkingsverantwoordelijke”.

Art. 23

In de artikelen 44/11/10 en 44/11/11 van dezelfde wet, ingevoegd bij de wet van 18 maart 2014, worden de

Les modalités de communication vers la police des données des services de renseignement sont déterminées dans un instrument juridique dont la date d’entrée en vigueur est simultanée à celle de l’accès direct des services de renseignement et de sécurité à la B.N.G.”.

Art. 22

À l’article 44/11/9 de la même loi, inséré par la loi du 18 mars 2014, les modifications suivantes sont apportées:

1° au paragraphe 1er, les 1° à 4°, sont remplacés par ce qui suit:

“1° la Cellule de traitement des informations financières;

2° l’Office des étrangers;

3° les services d’enquête et recherche et l’administration surveillance, contrôle et constatation de l’Administration générale des douanes et accises.”;

2° le paragraphe 2 est remplacé comme suit:

“§ 2. Selon les modalités déterminées par les directives des ministres de l’Intérieur et de la Justice, chacun dans le cadre de ses compétences, elles peuvent également être communiquées aux 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 lorsque ceux-ci en ont besoin pour l’exécution de leurs missions légales.

La liste de ces autorités, organes ou organismes est arrêtée par les ministres de l’Intérieur et de la Justice sur la base d’une proposition du Comité information et ICT visé à l’article 8*sexies* de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux.”.

3° au paragraphe 3, les mots “commissaire général de la police fédérale” sont remplacés par les mots “responsable du traitement”.

Art. 23

Aux articles 44/11/10 en 44/11/11 de la même loi, insérés par la loi du 18 mars 2014, les mots “la Commission

woorden “de Commissie voor de bescherming van de persoonlijke levenssfeer” vervangen door de woorden “het Controleorgaan”.

Art. 24

In artikel 44/11/12, § 1, van dezelfde wet, ingevoegd bij de wet van 18 maart 2014, worden de volgende wijzigingen aangebracht:

1° de woorden “de Commissie voor de bescherming van de persoonlijke levenssfeer” worden vervangen door de woorden “het Controleorgaan”;

2° in het 1° worden de woorden “in artikel 44/11/7 en 44/11/8” vervangen door de woorden “in artikelen 44/11/7, 44/11/8 en 44/11/8*bis*”.

Art. 25

In artikel 44/11/13, § 1, van dezelfde wet, ingevoegd bij de wet van 18 maart 2014, worden de volgende wijzigingen aangebracht:

1° de woorden “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” worden vervangen door de woorden “de bepalingen van Titel 2, Hoofdstuk V van de wet gegevensbescherming”;

2° de woorden “de Commissie voor de bescherming van de persoonlijke levenssfeer” worden vervangen door de woorden “het Controleorgaan”.

Art. 26

In artikel 46/1 van dezelfde wet, ingevoegd bij de wet van 21 maart 2018, worden de woorden “op de politionele informatie zoals bedoeld in artikel 44/6, hierna “Controleorgaan” genoemd,” geschrapt.

HOOFDSTUK II

Wijzigingen van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus

Art. 27

In titel I van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd

de la protection de la vie privée” sont remplacés par les mots “l’Organe de contrôle”.

Art. 24

À l’article 44/11/12, § 1er, de la même loi, inséré par la loi du 18 mars 2014, les modifications suivantes sont apportées:

1° les mots “la Commission de la protection de la vie privée” sont remplacés par les mots “l’Organe de contrôle”;

2° au 1°, les mots “à l’article 44/11/7 et 44/11/8” sont remplacés par les mots “aux articles 44/11/7, 44/11/8 et 44/11/8*bis*”.

Art. 25

À l’article 44/11/13, § 1er, de la même loi, inséré par la loi du 18 mars 2014, les modifications suivantes sont apportées:

1° les mots “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” sont remplacés par les mots “aux dispositions du Titre 2, Chapitre V, de la loi relative à la protection des données”;

2° les mots “la Commission de la protection de la vie privée” sont remplacés par les mots “l’Organe de contrôle”.

Art. 26

À l’article 46/1 de la même loi, inséré par la loi du 21 mars 2018, les mots “de l’information policière visé à l’article 44/6, ci-après dénommé “Organe de contrôle,”, sont supprimés.

CHAPITRE II

Modifications de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux

Art. 27

Au titre Ier de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux,

op twee niveaus wordt een hoofdstuk VI ingevoegd met als opschrift:

"Hoofdstuk VI. – Strategisch adviescomité voor informatie".

Art. 28

In hoofdstuk VI, ingevoegd door artikel 27, wordt een artikel 8*sexies* ingevoegd, luidende:

"Art. 8*sexies*. § 1. Er wordt een adviescomité opgericht dat belast is met de informatiestrategie en de ICT bij de geïntegreerde politie, "Comité Informatie en ICT" genoemd. Dit comité bestaat uit zes leden van de federale politie, zes leden van de lokale politie en van een vertegenwoordiger van de minister van Binnenlandse Zaken en van de minister van Justitie.

De functionaris voor gegevensbescherming die bij de commissaris-generaal wordt aangewezen, of zijn vertegenwoordiger, zetelt in het Comité Informatie en ICT in de hoedanigheid van deskundige.

Het Comité Informatie en ICT wordt gezamenlijk voorgezeten door de directeur-generaal van het middelenbeheer en de informatie, de federale politie en de voorzitter van de Vaste Commissie voor de lokale politie of hun afgevaardigde die respectievelijk lid zijn van de federale politie en de lokale politie bedoeld in het eerste lid.

§ 2. Het Comité Informatie en ICT is hetzij op eigen initiatief hetzij op vraag van het coördinatiecomité van de geïntegreerde politie, van de minister van Binnenlandse Zaken, van de minister van Justitie of van beiden via het coördinatiecomité van de geïntegreerde politie, van het directiecomité van de federale politie, van de Vaste Commissie voor de lokale politie of van een verwerkingsverantwoordelijke belast met het verstrekken van aanbevelingen en het verlenen van met redenen omklede adviezen aan hen over:

a) het beleid en de regelgeving betreffende het politioneel informatiebeheer, de informatie- en communicatiesystemen van de geïntegreerde politie;

b) het beleid van de informatiebeveiliging;

c) het beleid van de bescherming van gegevens en de beveiliging van de persoonsgegevens en hun verwerking.

Het coördinatiecomité van de geïntegreerde politie deelt het antwoord van het Comité Informatie en ICT

il est inséré un chapitre VI, intitulé comme suit:

"Chapitre VI. – Comité d'avis en charge de la stratégie en matière d'information".

Art. 28

Dans le chapitre VI, inséré par l'article 27, il est inséré un article 8*sexies*, rédigé comme suit:

"Art. 8*sexies*. § 1er. Il est institué un Comité d'avis en charge de la stratégie en matière d'information et d'ICT au sein de la police intégrée, dénommé "Comité Information et ICT". Ce comité est composé de six membres de la police fédérale, de six membres la police locale et d'un représentant du ministre de l'Intérieur et du ministre de la Justice.

Le délégué à la protection des données désigné auprès du Commissaire général ou son représentant siège en qualité d'expert au Comité Information et ICT.

Le Comité Information et ICT est co-présidé par le directeur général de la gestion des ressources et de l'information de la police fédérale et le président de la Commission permanente de la police locale ou leur délégué, qui font respectivement partie des membres de la police fédérale et de la police locale visés à l'alinéa 1er.

§ 2. Le Comité Information et ICT est chargé, soit d'initiative, soit à la demande du Comité de coordination de la police intégrée, du ministre de l'Intérieur, du ministre de la Justice ou des deux via le Comité de coordination de la police intégrée, du Comité de direction de la police fédérale, de la Commission permanente de la police locale ou d'un responsable du traitement de formuler des recommandations et de leur remettre des avis motivés relatifs à:

a) la politique et aux règles relatives à la gestion de l'information policière et aux systèmes d'information et de communication de la police intégrée;

b) la politique de sécurité de l'information;

c) la politique de protection des données et de sécurisation des données à caractère personnel et de leur traitement.

La réponse du Comité Information et ICT au ministre de l'Intérieur et au ministre de la Justice ou aux deux

mee aan de minister van Binnenlandse Zaken en de minister van Justitie of aan beiden.

Het Comité Informatie en ICT verstuurt jaarlijks een verslag naar de minister van Binnenlandse Zaken en de minister van Justitie betreffende de tenuitvoerlegging en uitvoering van de wettelijke en reglementaire bepalingen aangaande de politionele operationele gegevensverwerking en in het bijzonder betreffende de archivering en het wissen van gegevens die opgenomen zijn in de gegevensbanken bedoeld in artikel 44/2, § 1, tweede lid, 1° en 2°, van de wet op het politieambt. Dit verslag wordt eveneens overgemaakt aan het Controleorgaan bedoeld in artikel 71 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens de wet gegevensbescherming.

Het Comité Informatie en ICT onderzoekt de initiatieven genomen inzake politioneel informatiebeheer en de ontwikkeling van de systemen teneinde, in voorkomend geval, aanbevelingen te formuleren en gemotiveerde adviezen te verlenen.

Het Comité Informatie en ICT verleent eveneens advies, hetzij op eigen initiatief, hetzij op vraag van een verwerkingsverantwoordelijke, over elk voornemen om gegevens te verwerken dat het voorwerp was van uiteenlopende adviezen van functionarissen voor gegevensbescherming die onder verschillende, maar niet aan elkaar ondergeschikte overheden, vallen.

§ 3. Het Comité Informatie en ICT stelt een huishoudelijk reglement op dat de nadere regels voor de werking ervan vastlegt. Dit reglement wordt ter goedkeuring aan de ministers van Binnenlandse Zaken en Justitie voorgelegd.”.

§ 4. De adviezen van het Comité Informatie en ICT worden doorgegeven aan het Controleorgaan van de politionele informatie.”.

Art. 29

Titel V van dezelfde wet, opgeheven bij de wet van 15 mei 2007, wordt hersteld als volgt:

“Titel V – Modaliteiten betreffende de verwerking van persoonsgegevens”.

est communiquée par le Comité de coordination de la police intégrée.

Le Comité Information et ICT transmet annuellement au ministre de l’intérieur et au ministre de la justice un rapport quant à la mise en œuvre et l’exécution des dispositions légales et réglementaires relatives à la gestion de l’information policière opérationnelle et en particulier quant à l’archivage et à l’effacement des données contenues dans les banques de données visées à l’article 44/2, § 1er, alinéa 2, 1° et 2°, de la loi sur la fonction de police. Ce rapport est également transmis à l’Organe de contrôle visé à l’article 71 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnel.

Le Comité Information et ICT examine les initiatives prises en matière de gestion de l’information policière et de développement de systèmes pour formuler, le cas échéant, des recommandations et remettre des avis motivés.

Le Comité Information et ICT rend également un avis, d’initiative ou à la demande d’un responsable du traitement, concernant tout projet de traitement de données ayant fait l’objet d’avis divergents de délégués à la protection des données relevant d’autorités différentes, mais non subordonnées l’une à l’autre.

§ 3. Le Comité Information et ICT élabore un règlement d’ordre intérieur qui détermine les modalités de son fonctionnement. Ce règlement est soumis, pour approbation, aux ministres de l’Intérieur et de la Justice.”.

§ 4. Les avis du Comité Information et ICT sont transmis à l’Organe de contrôle de l’information policière. “.

Art. 29

Le titre V de la même loi, abrogé par la loi du 15 mai 2007, est rétabli sous l’intitulé suivant:

“Titre V – Modalités relatives au traitement de données à caractère personnel”.

Art. 30

In titel V van dezelfde wet, hersteld door artikel 29, wordt artikel 143, opgeheven bij de wet van 15 mei 2007, hersteld als volgt:

"Art. 143. Voor de toepassing van deze titel, verstaan we onder:

1° algemene verordening gegevensbescherming: de 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 de richtlijn 95/46/EG;

2° wet gegevensbescherming: de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.".

Art. 31

In titel V van dezelfde wet, hersteld door artikel 29, wordt artikel 144, opgeheven bij de wet van 15 mei 2007, hersteld als volgt:

"Art. 144. Elke verwerkingsverantwoordelijke en minstens elke politiezone, het commissariaat-generaal, elke algemene directie en elke directie van de federale politie wijst een of meerdere personeelsleden van de politie als functionaris voor gegevensbescherming aan overeenkomstig artikel 37 van de algemene verordening gegevensbescherming en artikel 63 van de wet gegevensbescherming.

Deze functionaris voor gegevensbescherming kan zijn functies uitoefenen voor verschillende lokale politiezones of voor verschillende directies, algemene directies en het commissariaat-generaal van de federale politie.

Hij oefent zijn taken volledig onafhankelijk uit.

De Koning bepaalt, overeenkomstig artikel 38.6 van de algemene verordening gegevensbescherming en artikelen 63, vijfde lid, en 64, zesde lid, van de wet gegevensbescherming de nadere regels betreffende de opdrachten en de werking van de functionaris voor gegevensbescherming.

Alle verwerkers die deelnemen aan de verwerking van persoonsgegevens ten behoeve van een verwerkingsverantwoordelijke of van één van de voormelde entiteiten van de geïntegreerde politie alsook elke overheid

Art. 30

Dans le titre V de la même loi, rétabli par l'article 29, l'article 143, abrogé par la loi du 15 mai 2007, est rétabli dans la rédaction suivante:

"Art. 143. Pour l'application du présent titre, on entend par:

1° règlement général sur la protection des données: 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;

2° loi relative à la protection des données: la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.".

Art. 31

Dans le titre V de la même loi, rétabli par l'article 29, l'article 144, abrogé par la loi du 15 mai 2007, est rétabli dans la rédaction suivante:

"Art. 144. Chaque responsable du traitement et au moins chaque zone de police, le commissariat général, chaque direction générale et chaque direction de la police fédérale désigne un ou plusieurs membres du personnel de la police en tant que délégué à la protection des données, conformément à l'article 37 du règlement général sur la protection des données et à l'article 63 de la loi relative à la protection des données.

Ce délégué à la protection des données peut exercer ses fonctions pour différentes zones de police locale ou différentes directions, directions générales et le commissariat général de la police fédérale.

Il exerce ses fonctions en toute indépendance.

Le Roi détermine, conformément à l'article 38.6 du règlement général sur la protection des données et aux articles 63, alinéa 5, et 64, alinéa 6 de la loi relative à la protection des données, les modalités relatives aux missions et au fonctionnement des délégués à la protection des données.

Tout sous-traitant participant au traitement de données à caractère personnel pour un responsable de traitement ou pour l'une des entités de la police intégrée précitées ainsi que chaque autorité ayant accès

die toegang heeft tot het communicatiesysteem of de gegevensverwerkingen door de politiediensten dienen eveneens een functionaris voor gegevensbescherming aan te duiden.".

Art. 32

In titel V van dezelfde wet, hersteld door artikel 29, wordt artikel 145, opgeheven bij de wet van 15 mei 2007, hersteld als volgt:

"Art. 145. Er wordt een uniek register van verwerkingsactiviteiten voor de geïntegreerde politie gecreëerd overeenkomstig artikel 30 van de algemene verordening gegevensbescherming en artikel 55 van de wet inzake gegevensbescherming.

De Koning bepaalt de vorm, de inhoud en de modaliteiten van het beheer van het register van verwerkingsactiviteiten.".

Art. 33

In titel V van dezelfde wet, hersteld door artikel 29, wordt artikel 146, opgeheven bij de wet van 15 mei 2007, hersteld als volgt:

"Art. 146. Alle verwerkingsverantwoordelijken van persoonsgegevens die door of krachtens de wet belast zijn met de toepassing van het statuut van de geïntegreerde politie delen aan elkaar de persoonsgegevens mee die behoren tot het toepassingsgebied van de algemene verordening gegevensbescherming en die noodzakelijk zijn voor de doeleinden die zij nastreven door of krachtens de wet.".

TITEL III

SLOTBEPALING

Art. 34

Artikel 284 van de wet gegevensbescherming is van toepassing op de artikelen 10, 4°, 11, 13, 4°, evenals artikel 14, 3°, voor wat betreft het tweede lid van paragraaf 4.

22 maart 2019

Franky DEMON (CD&V)
Veerle HEEREN (CD&V)
Katja GABRIËLS (Open Vld)
Sandrine DE CROM (Open Vld)

au système de communication ou aux traitements de données des services de police est également tenue de désigner un délégué à la protection des données.".

Art. 32

Dans le titre V de la même loi, rétabli par l'article 29, l'article 145, abrogé par la loi du 15 mai 2007, est rétabli dans la rédaction suivante:

"Art. 145. Il est créé un registre unique des activités de traitement pour la police intégrée, conformément à l'article 30 du règlement général sur la protection des données et à l'article 55 de la loi relative à la protection des données.

Le Roi détermine la forme, le contenu et les modalités de gestion du registre des activités de traitement.".

Art. 33

Dans le titre V de la même loi, rétabli par l'article 29, l'article 146, abrogé par la loi du 15 mai 2007, est rétabli dans la rédaction suivante:

"Art. 146. Tous les responsables de traitements de données à caractère personnel qui sont chargés par ou en vertu de la loi de l'application du statut de la police intégrée se communiquent les données à caractère personnel qui relèvent du champ d'application du règlement général sur la protection des données qui sont nécessaires à l'exercice de leurs missions.".

TITRE III

DISPOSITION FINALE

Art. 34

L'article 284 de la loi relative à la protection des données est applicable aux articles 10, 4°, 11, 13, 4°, ainsi qu'à l'article 14, 3°, pour ce qui concerne l'alinéa deux du paragraphe 4.

Centrale drukkerij – Imprimerie centrale