

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

17 april 2019

WETSVOORSTEL

**tot wijziging van diverse bepalingen wat het
politiebele informatiebeheer betreft**

VERSLAG VAN DE EERSTE LEZING

NAMENS DE COMMISSIE
VOOR DE BINNENLANDSE ZAKEN,
DE ALGEMENE ZAKEN
EN HET OPENBAAR AMBT
UITGEBRACHT DOOR
DE HEER **Christoph D'HAESE** EN
MEVROUW **Nawal BEN HAMOU**

INHOUD

Blz.

I. Procedure	3
II. Inleidende uiteenzetting van mevrouw Veerle Heeren, mede-indiener van het wetsvoorstel	3
III. Algemene bespreking.....	4
IV. Artikelsgewijze bespreking en stemmingen	8
Bijlagen	11

Zie:

Doc 54 **3697/ (2018/2019):**

- 001: Wetsvoorstel van de heer Demon en de dames Heeren, Gabriëls en De Crom.
002: Wijziging indiener.

Zie ook:

- 004: Artikelen aangenomen in eerste lezing.

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

17 avril 2019

PROPOSITION DE LOI

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

RAPPORT DE LA PREMIÈRE LECTURE

FAIT AU NOM DE LA COMMISSION
DE L'INTÉRIEUR,
DES AFFAIRES GÉNÉRALES
ET DE LA FONCTION PUBLIQUE
PAR
M. **Christoph D'HAESE** ET
MME **Nawal BEN HAMOU**

SOMMAIRE

Pages

I. Procédure	3
II. Exposé introductif Mme Veerle Heeren, co-auteur de la proposition de loi	3
III. Discussion générale.....	4
IV. Discussion des articles et votes	8
Annexes.....	11

Voir:

Doc 54 **3697/ (2018/2019):**

- 001: Proposition de loi de M. Demon et Mmes Heeren, Gabriëls et De Crom.
002: Modification auteur.

Voir aussi:

- 004: Articles adoptés en première lecture.

11303

**Samenstelling van de commissie op de datum van indiening van het verslag/
Composition de la commission à la date de dépôt du rapport**

Voorzitter/Président: Brecht Vermeulen

A. — Vaste leden / Titulaires:

N-VA Christoph D'Haese, Koenraad Degroote, Koen Metsu, Brecht Vermeulen
PS Nawal Ben Hamou, Julie Fernandez Fernandez, Eric Thiébaud
MR Sybille de Coster-Bauchau, Philippe Pivin, Françoise Schepmans
CD&V Franky Demon, Veerle Heeren
Open Vld Sandrine De Crom, Katja Gabriëls
sp.a Monica De Coninck
Ecolo-Groen Gilles Vanden Burre
cdH Vanessa Matz

B. — Plaatsvervangers / Suppléants:

Peter Buysrogge, Sarah Smeyers, Valerie Van Peel, Jan Vercammen, Bert Wollants
Laurent Devin, André Frédéric, Emir Kir, Laurette Onkelinx
Emmanuel Burton, Gautier Calomne, Caroline Cassart-Mailleux, Stéphanie Thoron
Wouter Beke, Leen Dierick, Nahima Lanjri
Patrick Dewael, Vincent Van Quickenborne, Frank Wilrycx
Hans Bonte, Alain Top
Wouter De Vriendt, Stefaan Van Hecke
Christian Brotcorne, Anne-Catherine Goffinet

C. — Niet-stemgerechtigde leden / Membres sans voix délibérative:

VB Filip Dewinter
DéFI Olivier Maingain
PP Aldo Carcaci

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-GOI	:	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 54^e 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 54^e 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

DAMES EN HEREN,

Uw commissie heeft dit wetsvoorstel besproken tijdens haar vergadering van 15 april 2019.

I. — PROCEDURE

Wetsvoorstel DOC 54 3697/001 was oorspronkelijk een wetsontwerp, dat uiteindelijk niet als dusdanig kon worden ingediend omdat de regering in lopende zaken was gegaan. Overeenkomstig de beslissing van de Conferentie van voorzitters heeft de bespreking plaatsgehad in aanwezigheid van de minister van Veiligheid en Binnenlandse Zaken.

Conform de beslissing van de Conferentie van voorzitters worden de beschikbare adviezen als bijlage bij dit verslag gevoegd. Het gaat om de respectieve adviezen van de Raad van State, van het Controleorgaan op de politionele informatie, van de Raad van burgemeesters, alsook van het College van procureurs-generaal.

II. — INLEIDENDE UITEENZETTING VAN MEVROUW VEERLE HEEREN, MEDE-INDIENER VAN HET WETSVORSTEL

Dit voorstel strekt ertoe om de wetgeving inzake het beheer van persoonsgegevens en van informatie door de politiediensten aan te passen aan de Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad. Daarnaast zijn bijkomende aanpassingen van de wet op het politieambt en van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus nodig voor de aanwijzing van het “controleorgaan op de politionele informatie” als gegevensbeschermingsautoriteit voor de politie.

In het belang van de geïntegreerde werking van de politie werd in het wetsvoorstel ervoor geopteerd om ook te voorzien in de oprichting van een Strategisch adviescomité voor informatie, het Strategisch Comité I, evenals in een uniek register van de verwerkingsactiviteiten voor de geïntegreerde politie.

MESDAMES, MESSIEURS,

Votre commission a examiné la présente proposition de loi au cours de sa réunion du 15 avril 2019.

I. — PROCÉDURE

La proposition de loi DOC 54 3697/001 était initialement un projet de loi que le gouvernement en affaires courantes n'a pu déposer comme projet de loi. Conformément à la décision de la Conférence des présidents, la discussion a eu lieu en présence du ministre de la Sécurité et de l'Intérieur.

Conformément à la décision de la Conférence des présidents, les avis disponibles sont joints en annexe au rapport. Il s'agit de l'avis du Conseil d'État, de l'avis de l'Organe de contrôle de l'Information policière, de l'avis du Conseil des bourgmestres ainsi que l'avis du Collège des procureurs généraux.

II. — EXPOSÉ INTRODUCTIF MME VEERLE HEEREN, CO-AUTEUR DE LA PROPOSITION DE LOI

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 (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil. Par ailleurs, il est nécessaire de procéder à des modifications complémentaires de la loi sur la fonction de police et de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux pour désigner “l'Organe de contrôle de l'information policière” comme autorité de protection des données pour la police.

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.

Aanvullend is het in de huidige realiteit van diverse samenwerkingsvormen tussen de verschillende politiediensten en toekomstige IT-ontwikkelingen die deze vormen van samenwerking ondersteunen (zoals i-Police) noodzakelijk om het kader inzake de koppeling van de diverse gegevensbanken verder te specificeren.

Ook de rechtstreekse toegang van de inlichtingendiensten tot de Algemene Nationale Gegevensbank (ANG) wordt in de wet ingeschreven overeenkomstig de aanbevelingen van de parlementaire onderzoekscommissie "Terroristische aanslagen" met betrekking tot een betere toegang tot informatie voor deze diensten. 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*. De nadere regels van deze wederkerigheid zal met alle relevante partners worden besproken.

Ten slotte worden 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 politimaatregel. Deze toevoeging is een gevolg van de operationele behoefte van de politiediensten om ANPR-camera's te kunnen inzetten, bij de effectieve opvolging van een politimaatregel, bevolen door een bevoegde overheid

III. — ALGEMENE BESPREKING

Mevrouw Nawal Ben Hamou (PS) stelt vast dat dit wetsvoorstel nu al tal van kritische reacties van allerlei organisaties heeft uitgelokt.

Het wetsvoorstel beoogt immers een ingrijpende wijziging van de regels inzake de toegang tot de Algemene nationale gegevensbank (ANG) en effent het pad voor een onderlinge koppeling van de bestaande databanken. Heikele gegevens, zoals die in verband met de gezondheid of met een eventuele bestuurlijke aanhouding, zullen voortaan kunnen worden verzameld.

De spreekster verwijst naar het advies van het Controleorgaan op de politionele informatie (COC), dat inhoudelijk een totaal andere strekking heeft dan het standpunt ter zake van de gewezen Commissie voor de bescherming van de persoonlijke levenssfeer.

Het lijkt haar dan ook heel belangrijk te kunnen beschikken over bijkomende adviezen, meer bepaald dat van het College van procureurs-generaal.

Il s'avère en outre nécessaire, dans la réalité actuelle des diverses formes de coopération entre les différents services de police 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.

L'accès direct à la Banque de Données nationale Générale (BNG) a également été inscrit dans la loi au profit des services de renseignement, conformément aux recommandations de la commission d'enquête parlementaire "Attentats terroristes" relatives à un meilleur accès à l'information pour ces services. Bien entendu, 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". Les modalités de cette réciprocité seront examinées avec tous les partenaires concernés.

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.

III. — DISCUSSION GÉNÉRALE

Mme Nawal Ben Hamou (PS) constate que la présente proposition de loi a d'ores et déjà suscité une série de réactions critiques de diverses organisations.

La proposition de loi modifie en effet radicalement les règles d'accès à la Banque de données nationale générale (BNG) et ouvre la possibilité d'une interconnexion entre les banques de données existantes. Des données sensibles, comme des données relatives à la santé, ou des informations concernant une éventuelle arrestation administrative pourront désormais être collectées.

L'intervenante se réfère à l'avis de l'Organe de contrôle de l'Information policière (COC) dont la teneur rompt totalement avec la position de l'ancienne Commission de la protection de la vie privée en la matière.

Il lui paraît dès lors essentiel de pouvoir disposer d'avis complémentaires et notamment de celui du Collège des procureurs généraux.

Aangaande de voorafgaande vormvereisten precieert mevrouw *Samuelle Godin*, lid van het ATS Justitie, dat de Raad van State in zijn advies geen fundamentele punten van kritiek uit, maar louter enkele technische opmerkingen formuleert. Zij bevestigt bovendien dat de ter bespreking voorliggende tekst wel degelijk werd voorgelegd aan het College van procureurs-generaal. Het College heeft een opmerking geformuleerd aangaande het wederkerigheidsaspect van de toegangen van de Veiligheid van de Staat. Daarentegen heeft het geen enkele opmerkingen geformuleerd over het operationeel beheer van de politionele informatie.

Aangaande de onderlinge koppeling van de politionele databanken herinnert de spreekster eraan dat er mettertijd meerdere (lokale en federale) databanken zijn opgericht.

De parlementaire onderzoekscommissie belast met het onderzoek naar de terroristische aanslagen heeft in haar aanbevelingen benadrukt dat alle relevante gegevens beschikbaar moeten worden gesteld voor de veiligheidsdiensten. De spreekster precieert dat die koppelingen zijn voorbehouden aan de leden van de politiediensten, met de bedoeling hen in staat te stellen hun taken doeltreffend te kunnen uitvoeren. Voorts verwijst zij naar Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad. Ze verwijst meer bepaald naar artikel 23 van die Richtlijn, dat luidt: “De lidstaten schrijven voor dat de verwerker en eenieder die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker en toegang heeft tot persoonsgegevens, deze uitsluitend volgens de instructies van de verwerkingsverantwoordelijke verwerkt, tenzij hij op grond van het Unierecht of het lidstatelijke recht tot de verwerking gehouden is”. In voorkomend zijn de verwerkingsverantwoordelijken de minister van Binnenlandse Zaken en de minister van Justitie, die de politiediensten dus richtsnoeren moeten geven. Voor die richtsnoeren gelden strikte nadere voorwaarden waarin wordt voorzien door het wetsvoorstel, dat duidelijke toegangprofielen vastlegt.

Aangaande de toegang van de inlichtingendiensten tot de Algemene nationale gegevensbank (ANG) heeft ook de spreekster kennis gekregen van de opmerkingen van de *Ligue des droits humains*. Zij verwijst van haar kant naar een brief van het Vast Comité I van 9 april 2019, waarin dat laatste betreurt dat de inlichtingendiensten

En ce qui concerne les formalités préalables, *Mme Samuelle Godin, membre du SAT Justice*, précise que dans son avis, le Conseil d’État ne formule pas de critiques fondamentales mais se limite à émettre quelques remarques techniques. Par ailleurs, elle confirme que le texte à l’examen a bel et bien été soumis au Collège des procureurs généraux. Le Collège a émis une remarque concernant l’aspect “réciprocité” des accès de la Sûreté de l’État. Il n’a par contre formulé aucune remarque concernant la gestion de l’information policière opérationnelle.

Concernant l’interconnexion des banques de données policières, l’intervenante rappelle qu’au cours des années, plusieurs banques de données (locales et fédérales) ont vu le jour.

La commission d’enquête parlementaire sur les Attentats terroristes a, dans ses recommandations, insisté sur la nécessité de mettre à disposition des services de sécurité l’ensemble des informations pertinentes. L’intervenante précise que ces interconnexions sont réservées aux membres des services de police afin de leur permettre de travailler de manière efficace. Elle se réfère par ailleurs à la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d’enquêtes et de poursuites en la matière ou d’exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil et en particulier à son article 23 selon lequel: “Les États membres prévoient que le sous-traitant et toute personne agissant sous l’autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite que sur instruction du responsable du traitement, à moins d’y être obligé par le droit de l’Union ou le droit d’un État membre”. En l’occurrence, les responsables du traitement sont les ministres de l’Intérieur et de la Justice, lesquels sont donc tenus de donner des directives aux services de police. Ces directives sont strictement encadrées par les dispositions de la proposition de loi qui définit clairement les profils d’accès.

En ce qui concerne l’accès des services de renseignement à la banque de données nationale générale (BNG), l’intervenante a pris, elle aussi, connaissance des observations formulées par la Ligue des Droits humains. Elle se réfère, pour sa part, à un courrier du Comité permanent R du 9 avril 2019 dans lequel ce

nog steeds geen rechtstreekse toegang tot de ANG hebben en ervoor pleit dat de nodige maatregelen worden genomen om dat euvel te verhelpen. Uit operationeel oogpunt gaat het hier om een essentieel element. Het is hoegenaamd niet de bedoeling de inlichtingendiensten onbeperkte toegang tot alle politionele databanken te verlenen, maar wel hun louter toegang te verschaffen tot de ANG. Tot dusver was slechts een rechtstreekse bevraging toegestaan. Daarbij kon alleen informatie worden opgevraagd voor een welbepaalde persoon en voor de feiten waarvoor die laatste gekend is. Bij een rechtstreekse toegang, daarentegen, kan toegang worden verkregen tot het relationele model dat aan de ANG ten grondslag ligt. Daarbij kan informatie worden verkregen met betrekking tot andere feiten of tot andere personen die in verband worden gebracht met de feiten waarvoor de betrokkene gekend is. Het spreekt vanzelf dat die rechtstreekse toegang essentieel is voor de inlichtingendiensten. Niettemin zal die toegang slechts worden verleend binnen het raam van de uitoefening van hun wettelijke taken. Strikte criteria in verband met die toegang zullen worden bepaald bij een koninklijk besluit vastgesteld na overleg in de Ministerraad.

Zoals de *Ligue des droits humains* in herinnering heeft gebracht, bevat de ANG uiteraard niet alleen informatie over dreigingen in verband met de veiligheid, maar ook over gewone criminaliteit. Zoals de werkzaamheden van de onderzoekscommissie belast met het onderzoek naar de terroristische aanslagen duidelijk hebben gemaakt, is de grens tussen gewone criminaliteit en dreigingen in verband met de veiligheid soms heel dun. De daders van de aanslagen in Brussel waren immers gekend voor "traditionele" criminele feiten.

Omgekeerd kan de toegang tot die informatie ook à *décharge* worden aangewend. Mevrouw Godin geeft het voorbeeld van een persoon die banden heeft met de geradicaliseerde milieus over wie de inlichtingendiensten te weten waren gekomen dat hij aan precursoren (stoffen die worden gebruikt voor de productie van een bom) trachtte te raken. Logischerwijs konden die diensten aannemen dat die persoon een aanslag aan het voorbereiden was. Uit een bevraging van de politiediensten is gebleken dat die persoon ook bekend stond voor drugshandel. Na onderzoek werd duidelijk dat de zoektocht naar precursoren geen verband hield met het voorbereiden van een eventuele aanslag, maar wel met de productie van synthetische drugs.

De spreekster wijst erop dat de door het wetsvoorstel beoogde rechtstreekse toegang de basisbeginselen inzake gegevensbescherming in acht neemt. Alle raadplegingen worden geregistreerd en kunnen door de bevoegde gegevensbeschermingsautoriteit, met name het Vast Comité I, worden gecontroleerd.

dernier déplore que les services de renseignement n'ont toujours pas d'accès direct à la BNG et plaide pour que les mesures nécessaires soient prises afin de remédier à ce problème. Il s'agit d'un élément essentiel d'un point de vue opérationnel. Il n'est ici nullement question de donner aux services de renseignement un accès illimité à l'ensemble des banques de données policières mais seulement de leur permettre d'avoir accès à la BNG. Jusqu'à présent, seule une interrogation directe était autorisée. Celle-ci ne permet d'obtenir des informations que sur une personne déterminée et les faits pour lesquels celle-ci est connue. L'accès direct, par contre, permet d'avoir accès au modèle relationnel à la base de la BNG. Il permet d'obtenir des informations concernant d'autres faits ou d'autres personnes liés aux faits pour lesquels la personne concernée est connue. Il est évident que cet accès direct est essentiel aux services de renseignement. Cela étant, cet accès ne leur est conféré que dans le cadre de leurs missions légales. Un arrêté royal délibéré en Conseil des ministres fixera des critères stricts pour encadrer cet accès.

Certes, comme la Ligue des Droits humains le rappelle, la BNG ne contient pas seulement des informations relatives aux menaces pour la sécurité mais aussi des informations concernant la criminalité ordinaire. Comme l'ont démontré les travaux de la commission d'enquête sur les Attentats terroristes, le lien entre la criminalité ordinaire et les menaces contre la sécurité est parfois ténu. Les auteurs des attentats de Bruxelles étaient en effet connus pour des faits de criminalité "classique".

A l'inverse, l'accès à ces informations peut également être utilisé à *décharge*. Mme Godin cite à titre d'illustration le cas d'une personne liée aux milieux radicalisés dont les services de renseignement avaient appris qu'elle tentait d'obtenir des précurseurs (utilisés pour la fabrication d'une bombe). Ils pouvaient donc logiquement penser que cette personne préparait un attentat. En interrogeant les services de police, il est apparu que cette personne était également connue pour trafic de drogues. Après enquête, il est devenu clair que la recherche de ces précurseurs n'était pas liée à la préparation d'un attentat éventuel, mais bien à la fabrication de drogues synthétiques.

L'intervenante rappelle que l'accès direct, tel que conféré par la proposition de loi, respecte les principes de base en matière de protection des données. Toutes les consultations sont enregistrées et pourront faire l'objet d'un contrôle par l'autorité de protection des données compétente, à savoir le Comité permanent R.

Aangaande de gevoelige gegevens waarnaar mevrouw Ben Hamou heeft verwezen, benadrukt mevrouw Godin dat het wetsvoorstel de loutere omzetting van de bepalingen van de AVG beoogt. Dergelijke gegevens worden nooit losstaand behandeld, maar altijd in het kader van de opdrachten van de politiediensten. Het wetsvoorstel moet overigens worden gelezen in het licht van de kaderwet betreffende de gegevensbescherming en in het bijzonder van Titel 2 ervan. Niettemin beoogt dit wetsvoorstel te voorzien in bijkomende voorwaarden (het toegangprofiel moet worden meegedeeld aan de toezichthoudende autoriteit en de vertrouwelijkheid van de gegevens moet worden gewaarborgd). Het wetsvoorstel maakt ook een onderscheid naargelang de hoedanigheid van de persoon wiens gegevens worden geraadpleegd (betreft het een verdachte, een getuige, een slachtoffer?).

Voorts strekt het wetsvoorstel tot het opleggen van een actief veiligheidsbeleid inzake die gegevens, waarbij elke verwerkingsverantwoordelijke een gegevensbeschermingsplan zou moeten opstellen. Ten slotte is het de bedoeling dat een specifieke instantie, het COC, belast is met het toezicht.

Mevrouw Godin voegt eraan toe dat alle verwerkingen in de ANG gedurende dertig jaar in logbestanden zouden worden bijgehouden. Tijdens die periode kan de politiebeambte worden gevraagd te verantwoorden waarom hij de gegevens heeft geraadpleegd.

De heer Philippe Pivin (MR) stelt vast dat de antwoorden van mevrouw Godin een en ander hebben verduidelijkt.

Dit wetsvoorstel houdt rekening met de adviezen van de Raad van State en van het Controleorgaan op de politieke informatie en strookt met de aanbevelingen van de parlementaire onderzoekscommissie "Terroristische aanslagen", wat de uitwisseling van informatie betreft. Ook het Vast Comité I is voorstander van de voorgestelde maatregel. Al deze aspecten in acht genomen, kondigt de spreker aan dat zijn fractie dit wetsvoorstel zal steunen.

Ook *mevrouw Veerle Heeren (CD&V)* herinnert eraan dat de voornoemde parlementaire onderzoekscommissie eenparig de oprichting van een "kruispuntbank veiligheid" had aanbevolen. Dit wetsvoorstel zou een eerste stap zijn en zou de informatie-uitwisseling, uiteraard met inachtneming van strikte voorwaarden, ten goede komen.

Concernant les données sensibles auxquelles Mme Ben Hamou s'est référée, Mme Godin souligne que la proposition de loi ne fait que transposer les dispositions du RGPD. Ce sont des données qui ne sont jamais traitées seules mais bien en lien avec les missions des services de police. Il convient d'ailleurs de lire le texte à la lumière de la loi-cadre en matière de protection des données et en particulier de son titre 2. La proposition de loi à l'examen prévoit toutefois des verrous supplémentaires (profil d'accès à transmettre à l'Autorité de contrôle et garantie de confidentialité des données). Le texte fait également une distinction selon la qualité de la personne faisant l'objet de la consultation (s'agit-il d'un suspect, d'un témoin, d'une victime?).

Par ailleurs, le texte impose une politique de sécurité active au niveau de ces données, chaque responsable du traitement étant chargé de faire un plan en matière de protection des données. Enfin, un organe spécifique, le COC, est chargé du contrôle.

Mme Godin ajoute encore que tous les traitements réalisés dans la B.N.G. feront l'objet d'une journalisation qui sera conservée pendant trente ans à partir du traitement. Pendant cette durée, le policier est donc susceptible de devoir rendre des comptes quant aux motifs de la consultation.

M. Philippe Pivin (MR) constate que les réponses de Mme Godin ont permis de clarifier les choses.

Le texte à l'examen tient compte des avis du Conseil d'État et de l'Organe de contrôle de l'Information policière et est conforme aux recommandations de la commission d'enquête parlementaire "Attentats terroristes" relatives au partage d'information. Le Comité permanent R s'est également prononcé en faveur de la mesure en projet. Compte tenu de l'ensemble de ces éléments, l'intervenant annonce que son groupe politique apportera son soutien à la proposition de loi à l'examen.

Mme Veerle Heeren (CD&V) rappelle, elle aussi, qu'à l'unanimité de ses membres, la commission d'enquête parlementaire précitée avait recommandé la création d'une Banque-carrefour de la Sécurité. La proposition de loi à l'examen est une première étape et favorisera le partage de l'information, moyennant évidemment le respect de conditions strictes.

IV. — ARTIKELSGEWIJZE BESPREKING EN STEMMINGEN

TITEL I

Algemene bepaling

Artikel 1

Dit artikel bepaalt de constitutionele grondslag van het wetsvoorstel. Er worden geen opmerkingen over gemaakt.

Het wordt eenparig aangenomen.

TITEL II

Wijzigingsbepalingen

HOOFDSTUK I

Wijzigingen van de wet op het politieambt

Art. 2 en 3

Over deze artikelen worden geen opmerkingen gemaakt.

Ze worden achtereenvolgens aangenomen met 11 stemmen en 2 onthoudingen.

Art. 4

Over dit artikel worden geen opmerkingen gemaakt.

Het wordt aangenomen met 11 stemmen tegen 1 en 1 onthouding.

Art. 5 en 6

Over deze artikelen worden geen opmerkingen gemaakt.

Ze worden achtereenvolgens aangenomen met 11 stemmen en 2 onthoudingen.

Art. 7

Over dit artikel worden geen opmerkingen gemaakt.

Het wordt aangenomen met 11 stemmen tegen 1 en 1 onthouding.

IV. — DISCUSSION DES ARTICLES ET VOTES

TITRE I^{ER}

Disposition générale

Article 1^{er}

Cet article qui définit la base constitutionnelle de la proposition de loi ne donne lieu à aucun commentaire.

Il est adopté à l'unanimité.

TITRE II

Dispositions modificatives

CHAPITRE I^{ER}

Modifications de la loi sur la fonction de police

Art. 2 et 3

Ces articles n'appellent aucun commentaire.

Ils sont successivement adoptés par 11 voix et 2 abstentions.

Art. 4

Cet article ne donne lieu à aucune observation.

Il est adopté par 11 voix contre une et une abstention.

Art. 5 et 6

Ces articles n'appellent aucun commentaire.

Ils sont successivement adoptés par 11 voix et 2 abstentions.

Art. 7

Cet article ne donne lieu à aucune observation.

Il est adopté par 11 voix contre une et une abstention.

Art. 8 tot 19

Over deze artikelen worden geen opmerkingen gemaakt.

Ze worden achtereenvolgens aangenomen met 11 stemmen en 2 onthoudingen.

Art. 20

Over dit artikel worden geen opmerkingen gemaakt.

Het wordt aangenomen met 11 stemmen tegen 1 en 1 onthouding.

Art. 21 tot 26

Over deze artikelen worden geen opmerkingen gemaakt.

Ze worden achtereenvolgens aangenomen met 11 stemmen en 2 onthoudingen.

HOOFDSTUK II

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

Art. 27 tot 33

Over deze artikelen worden geen opmerkingen gemaakt.

Ze worden achtereenvolgens aangenomen met 11 stemmen en 2 onthoudingen.

TITEL III

Slotbepaling

Art. 34

Over dit artikel worden geen opmerkingen gemaakt.

Het wordt aangenomen met 11 stemmen en 2 onthoudingen.

Op verzoek van de mevrouw Nawal Ben Hamou (PS) zal de commissie, overeenkomstig artikel 83.1 van het

Art. 8 à 19

Ces articles n'appellent aucun commentaire.

Ils sont successivement adoptés par 11 voix et 2 abstentions.

Art. 20

Cet article ne donne lieu à aucune observation.

Il est adopté par 11 voix contre une et une abstention.

Art. 21 à 26

Ces articles n'appellent aucun commentaire.

Ils sont successivement adoptés par 11 voix et 2 abstentions.

CHAPITRE II

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

Art. 27 à 33

Ces articles n'appellent aucun commentaire.

Ils sont successivement adoptés par 11 voix et 2 abstentions.

TITRE III

Disposition finale

Art. 34

L'article 34 n'appelle aucun commentaire.

Il est adopté par 11 voix et 2 abstentions.

A la demande de Mme Nawal Ben Hamou (PS), la commission procédera, conformément à l'article 83.1

Reglement van de Kamer van volksvertegenwoordigers, overgaan tot een tweede lezing van de aangenomen artikelen.

De commissie wenst daartoe te beschikken over een nota van de Juridische Dienst.

De rapporteurs,

De voorzitter,

Christoph D'HAESE

Brecht VERMEULEN

Nawal BEN HAMOU

Bepalingen die een uitvoeringsmaatregel vergen (artikel 78.2, vierde lid, van het Reglement): *niet meegedeeld*.

du Règlement de la Chambre des représentants, à une deuxième lecture des articles adoptés.

La commission souhaite disposer à cet effet d'une note du Service juridique.

Les rapporteurs,

Le président,

Christoph D'HAESE

Brecht VERMEULEN

Nawal BEN HAMOU

Dispositions nécessitant une mesure d'exécution (article 78.2, alinéa 4, du Règlement): *non communiqué*.

ANNEXES - BIJLAGEN



CONSEIL D'ÉTAT
section de législation

RAAD VAN STATE
afdeling Wetgeving

avis 65.312/2
du 4 mars 2019

advies 65.312/2
van 4 maart 2019

sur

over

un avant-projet de loi 'relatif à
la gestion de l'information
policière et modifiant la loi sur
la fonction de police et la loi
du 7 décembre 1998 organisant
un service de police intégré,
structuré à deux niveaux'

een voorontwerp van wet
'betreffende het politionele
informatiebeheer en tot
wijziging van de wet op het
politieambt en de wet van
7 december 1998 tot
organisatie van een
geïntegreerde politiedienst,
gestructureerd op
twee niveaus'

Comme la demande d'avis est introduite sur la base de l'article 84, § 1^{er}, alinéa 1^{er}, 2^o, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, la section de législation limite son examen au fondement juridique de l'avant-projet[‡], à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, l'avant-projet appelle les observations suivantes.

FORMALITÉ PRÉALABLE

L'avis n° 009/2018 de l'Organe de contrôle de l'information policière a été donné le 12 décembre 2018 sur l'avant-projet de loi soumis au Conseil d'État.

Cet avis a été communiqué à la section de législation en néerlandais. Il résulte de la demande formulée auprès de la fonctionnaire déléguée qu'il n'existe pas de version française.

L'Organe de contrôle de l'information policière (ci-après : le « C.O.C. ») a été créé par l'article 71 de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel' auprès de la Chambre des représentants. Il doit être consulté en application de l'article 59, § 1^{er}, alinéa 2, de la même loi « 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 (des données à caractère personnel) »¹.

L'article 4, § 2, alinéa 4, de la loi du 3 décembre 2017 'portant création de l'Autorité de protection des données' prévoit qu'« [à] l'égard des services de police au sens de l'article 2, 2^o, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle de l'information policière visé à l'article 44/6, § 1^{er}, de la loi du 5 août 1992 sur la fonction de police ». Pour les services de police, il y a lieu de faire également référence à l'article 19 de la loi du 30 juillet 2018².

[‡] S'agissant d'un avant-projet de loi, on entend par « fondement juridique » la conformité aux normes supérieures.

¹ Cette disposition figure dans le titre 2 de cette loi (« De la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces »).

² Cette disposition figure dans le titre 1^{er} de cette loi (« De la protection des personnes physiques à l'égard du traitement des données à caractère personnel »).

BNG, le transfert international des données, les délais de conservation des données, etc... À chaque fois, la Cour renvoyait au contrôle par l'Organe de contrôle afin de justifier la constitutionnalité de ces dispositions.

Le rôle important que l'Organe de Contrôle joue dans l'actuel système de gestion de l'information policière et même plus général dans toute l'architecture de la sécurité, était mis en avant par la commission d'enquête parlementaire 'chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste' (ci-après 'CEP Attentats') et plus particulièrement dans son 3^{ème} rapport intermédiaire sur le volet architecture de la sécurité (*Doc. parl.*, Chambre, 2016-2017, n° 1752/008). Le sujet de l'information (policière) était un des thèmes centraux dans les travaux de la CEP (voir principalement le chapitre IV, 'La gestion des informations'). [...] »⁴.

Dès lors que les avis du C.O.C., tels que l'avis n° 009/2018 du 12 décembre 2018, conformément à l'article 59, § 1^{er}, alinéa 2, de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel', sont conçus comme s'inscrivant « dans le cadre [notamment] de l'élaboration d'une loi » et que l'importance de l'intervention du C.O.C. a été expressément soulignée tant par la Cour constitutionnelle, statuant au contentieux des droits et libertés fondamentaux, que par l'exposé des motifs du projet devenu cette loi du 30 juillet 2018, il ne se conçoit pas que l'avis ne soit pas émis tant en néerlandais qu'en français⁵.

Par ailleurs, le texte de l'avant-projet sur lequel porte la demande d'avis introduite auprès de la section de législation du Conseil d'État n'a pas été modifié consécutivement à l'avis du C.O.C. Afin d'éviter que le Conseil d'État donne un avis sur un texte qui n'est pas définitif au stade de l'avant-projet précédant l'adoption du projet soumis à la Chambre des représentants, il est recommandé de ne soumettre au Conseil d'État un avant-projet de loi qu'à l'issue des différentes étapes de la préparation administrative de l'avant-projet.

Il serait opportun en outre que l'exposé des motifs fournisse des éclaircissements quant à la manière dont l'avis du C.O.C. aura été pris en compte par le projet.

OBSERVATIONS GÉNÉRALES

A. Modifications liées à l'évolution du cadre juridique européen et belge

L'avant-projet a notamment pour objet de modifier la loi du 5 août 1992 'sur la fonction de police', spécialement ses articles 3, 25/8, plusieurs articles contenus entre l'article 44/1 et l'article 44/11/13, ainsi que son article 46/1.

L'objectif poursuivi par l'auteur de l'avant-projet est de transposer, pour le volet opérationnel, la directive n° 2016/680 du Parlement européen et du Conseil du 27 avril 2016

⁴ *Doc. parl.*, Chambre, 2017-2018, n° 54-3126/001, pp. 115 à 118.

⁵ Il est rappelé qu'en vertu de l'article 231, § 1^{er}, de la loi du 30 juillet 2018, le C.O.C. est organisé de manière à assurer son bilinguisme.

Les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne ont, en ce qui concerne le traitement des données à caractère personnel dans le cadre de la mise en œuvre du droit de l'Union, une portée analogue à celle de l'article 8 de la Convention européenne des droits de l'homme et de l'article 22 de la Constitution. Il en va de même de l'article 17 du Pacte international relatif aux droits civils et politiques.

Le droit au respect de la vie privée, tel qu'il est garanti par les dispositions constitutionnelles et conventionnelles précitées, a pour but essentiel de protéger les personnes contre les ingérences dans leur vie privée. Ce droit a une portée étendue et englobe notamment la protection des données à caractère personnel et des informations personnelles.

À cet égard et en ce qui concerne les domaines d'application en dehors de l'Union européenne, la Convention n° 108 du Conseil de l'Europe 'pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel', qui lie l'État belge, impose également une série de garanties minimales à l'État belge.

2.1. Ce droit n'est cependant pas absolu. Il n'exclut pas toute ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée mais il est requis qu'elle soit prévue par une disposition législative suffisamment précise, qu'elle réponde à un besoin social impérieux dans une société démocratique et qu'elle soit proportionnée à l'objectif légitime qu'elle poursuit. Ces dispositions engendrent de surcroît l'obligation positive, pour l'autorité publique, de prendre des mesures qui assurent le respect effectif de la vie privée, même dans la sphère des relations entre les individus.

2.2. En réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée, l'article 22 de la Constitution garantit à tout citoyen qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue. Une délégation à un autre pouvoir n'est toutefois pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur.

2.3. Outre l'exigence de légalité formelle, l'article 22 de la Constitution impose également que l'ingérence dans l'exercice du droit au respect de la vie privée soit définie en des termes clairs et suffisamment précis qui permettent d'appréhender de manière prévisible les hypothèses dans lesquelles le législateur autorise une pareille ingérence.

De même, l'exigence de prévisibilité à laquelle la loi doit satisfaire pour être jugée conforme à l'article 8 de la Convention européenne des droits de l'homme implique que sa formulation soit assez précise pour que chacun puisse – en s'entourant au besoin de conseils éclairés – prévoir, à un degré raisonnable, dans les circonstances de la cause, les conséquences d'un acte déterminé. La législation doit donner à chacun une indication suffisante sur les circonstances dans lesquelles et à quelles conditions elle habilite la puissance publique à recourir à des mesures affectant les droits protégés par la Convention. Plus particulièrement, lorsque l'intervention de l'autorité présente un caractère secret, la loi doit offrir des garanties suffisantes contre les ingérences arbitraires dans l'exercice du droit au respect de la vie privée, en délimitant le pouvoir d'appréciation des autorités concernées avec une netteté suffisante, d'une part, et en prévoyant des procédures qui permettent un contrôle effectif, d'autre part.

Il découle dès lors de l'article 8 de la Convention et de l'article 22 de la Constitution qu'il doit être prévu de manière suffisamment précise dans quelles circonstances un traitement de données à caractère personnel est autorisé. Le niveau requis de précision de la législation concernée – laquelle ne peut du reste parer à toute

2. L'avant-projet sera complété par une disposition nouvelle mentionnant la transposition de la directive n° 2016/680, conformément à son article 63, paragraphe 1, alinéa 2.

Article 2

Dans la version française de l'article 2, 1°, de l'avant-projet, ce sont les mots « article 36ter de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard du traitement des données à caractère personnel » qui doivent être remplacés par les mots « article 71 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ».

Article 4

1. Compte tenu de l'usage de la notion de données « sensibles » à l'article 44/1, § 2, alinéa 1^{er}, en projet de la loi du 30 juillet 2018, il y a lieu d'insérer dans l'avant-projet une disposition complétant l'article 3 de la loi du 5 août 1992 qui aura pour objet de définir cette notion de données sensibles, et ce en transposant l'article 10 de la directive n° 2016/680, laquelle utilise la notion de « catégories particulières de données à caractère personnel »¹⁰.

2. À l'alinéa 7 du paragraphe 2 en projet, il est mentionné que « [l]e Roi peut prévoir d'autres garanties appropriées ».

Il ne serait pas admissible que cette habilitation au Roi Lui permette de substituer d'autres garanties à celles prévues par l'alinéa 6 en projet du même paragraphe 2. Le commentaire de l'article 4 de l'avant-projet ne contient aucune précision à ce sujet.

La disposition doit être revue de manière à prévoir que ces « autres garanties » ne peuvent être que complémentaires à celles énoncées à cet alinéa 6 en projet.

Article 7

1. L'article 7 de l'avant-projet dispose que les ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences, déterminent par « directives » les mesures nécessaires en vue d'assurer la gestion et la sécurité des données à caractère personnel et des informations traitées dans les banques de données visées à l'article 44/2 (article 44/4, § 2, alinéa 1^{er}, en projet de la loi du 5 août 1992), les règles d'accès des membres des services de police aux banques de données visées à l'article 44/2, § 1^{er} et § 3 (article 44/4, § 3, en projet de la loi du 5 août 1992), et 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 (article 44/4, § 3bis, alinéa 1^{er}, en projet de la loi du 5 août 1992) et 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

¹⁰ En ce sens l'avis n° 009/2018 du 12 décembre 2018, au point 4.

Si le principe de légalité qui sous-tend le droit au respect de la vie privée n'interdit pas toute délégation à un autre niveau de pouvoir, une telle délégation n'est admissible qu'à la condition que celle-ci soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur.

A fortiori, il n'est pas envisageable que les modalités des garanties mises en place afin d'encadrer la limitation du droit à la vie privée apportée par le traitement de données à caractère personnel soient fixées dans un texte dépourvu de caractère contraignant et, par voie de conséquence, de la prévisibilité et de la sécurité juridique qui s'imposent.

En outre, les articles 33 et 108 de la Constitution s'opposent à ce que le législateur attribue directement certaines missions d'exécution à un ministre. Il appartient en effet au pouvoir exécutif de régler le fonctionnement et l'organisation de ses services. La loi doit habiliter le Roi à effectuer les différentes tâches visées, celui-ci pouvant éventuellement les déléguer lui-même ».

Ces observations valent en l'espèce pour l'article 44/4, § 2, alinéas 1^{er}, 5, 6, 8 et 9, § 3, § 3bis et § 4, en projet de la loi du 5 août 1992.

L'article 7 de l'avant-projet sera revu en conséquence.

2. Les alinéas 2 à 4 du paragraphe 2 en projet reproduisent en substance l'article 56 de la loi du 30 juillet 2018.

Il n'est pas adéquat du point de vue légistique de procéder de la sorte.

Il est en effet peu heureux qu'un dispositif soit doublement localisé dans l'ordonnancement juridique et ce, d'autant moins qu'en cas de modification de l'un de ces deux dispositifs sans apporter de modification à l'autre, une discordance éventuellement non voulue pourrait apparaître.

Le recours à pareille technique est d'autant moins indiqué que, par exemple, à l'alinéa 6 du même paragraphe 2 en projet, il est à bon escient procédé par renvoi à la loi du 30 juillet 2018.

Article 8

1. Il y a lieu de préciser, au 1^o, que c'est l'alinéa 1^{er} du paragraphe 1^{er} de l'article 44/5 qui est complété.

2. Dans son avis n° 009/2018 du 12 décembre 2018, au point 9, le C.O.C. estime qu'il faut non seulement viser les données relatives aux personnes faisant l'objet d'une mesure administrative mais aussi celles relatives aux personnes faisant l'objet d'une sanction administrative prise par une autorité administrative compétente et que les services de police sont chargées de suivre en vertu de la loi (article 44/5, § 1^{er}, alinéa 1^{er}, 7^o, en projet de la loi du 5 août 1992).

Le commentaire de l'article rejoint l'avis du C.O.C. sur ce point.

Interrogée sur le fait que la création des banques de données particulières ne doit pas se faire sur avis de l'Organe de contrôle mais que celui-ci est « averti activement, via le registre », la fonctionnaire déléguée a fourni les explications suivantes :

« Pour ce qui concerne les déclarations préalables des banques de données particulières au COC. Le COC indique lui-même dans son avis qu'il pourrait rendre un avis sur la base de l'accès direct qui lui serait fourni dans le registre des traitements et de la fonction alarme (il sera activement prévenu lorsqu'une nouvelle banque de données sera déclarée dans via ce registre). Il déclare lui-même que beaucoup de banques de données particulières sont en fait non sensibles. Dès lors obtenir un aval via un envoi séparé de ce registre ne représente pas beaucoup de plus-value. Rien n'empêche bien entendu le COC d'utiliser son pouvoir issu de l'article 59 de la loi cadre protection des données pour demander un accord sur certaines catégories de banques de données particulières comme par exemple celles pour lesquelles il y aurait recours à de nouvelles technologies (on peut penser par exemple au 'facial recognition'). Je me permets de recadrer cette discussion dans l'ensemble du package de la loi cadre protection des données : pas mal de législations prévoyaient ce mécanisme de déclaration préalable vers la Commission de la protection de la vie privée. Cette dernière est intervenue pour y mettre fin car cela ne correspondait selon elle plus du tout aux principes du [RGPD] où le responsable du traitement est celui qui porte la responsabilité finale et doit pouvoir démontrer qu'il respecte les règles du [RGPD] »¹⁵.

Ce complément d'informations pourrait figurer dans le commentaire de l'article 14.

Article 15

L'auteur de l'avant-projet doit vérifier les modifications prévues à l'article 44/11/3*bis* de la loi du 5 août 1992.

Ainsi, dans la version française, les mots « l'Organe de contrôle » doivent être remplacés par le mot « Organe ». Dans la version néerlandaise, on écrira de même « het orgaan » plutôt que « het controleorgaan ».

Ensuite, il y a lieu de lire, dans la version française de l'article 15, 2°, de l'avant-projet, « du délégué à la protection des données [...] ». Cette dernière observation vaut également pour l'article 44/11/3*quinqüies*/1, alinéa 1^{er}, en projet de la loi du 5 août 1992.

Article 16

L'auteur de l'avant-projet doit vérifier si certaines missions du délégué à la protection des données, qui sont énumérées complémentaires et qui sont reprises de l'article 44/3, § 1^{er}, alinéa 5, de la même loi (anciennes missions du conseiller en sécurité), ne correspondent pas en partie aux missions contenues dans l'article 65 de la loi du 30 juillet 2018.

¹⁵ Voir l'avis du C.O.C. n° 009/2018 du 12 décembre 2018, au point 12, *in fine*.

Article 27

À l'article 8^{sexies}, § 1^{er}, alinéa 3, en projet de la loi du 7 décembre 1998 'organisant un service de police intégré, structuré à deux niveaux', il n'apparaît pas clairement si les co-présidents désignés par cet alinéa font ou non partie des quatorze membres qui composent le comité en vertu de l'alinéa 1^{er} de la même disposition.

La disposition à l'examen sera clarifiée.

Article 33

Il ressort du commentaire de l'article 33 de l'avant-projet ce qui suit :

« Cet article prévoit une protection des données opérationnelles (traitées en application de la loi relative à la protection des données) en cas de traitement *interne à la police* de ces données, soumis au RGPD. Cette disposition vise à éviter que des données opérationnelles ne soient consultables par la personne concernée grâce à un accès direct dans le cadre d'un traitement administratif des données opérationnelles (p. ex. l'enquête de moralité effectuée dans le cadre de la procédure de recrutement).

Cet article ayant été conçu par analogie avec l'article 14 de la loi relative à la protection des données, il peut être fait référence sur ce point à l'exposé des motifs de la loi relative à la protection des données (*Doc. parl.*, 54K3126001, 36-39) ».

L'article 33 de l'avant-projet (article 147 en projet de la loi du 7 décembre 1998) reproduit en grande partie l'article 14 de la loi du 30 juillet 2018.

Une telle façon de légiférer est fortement déconseillée, d'autant plus qu'il s'agit de la mise en œuvre de l'article 23, paragraphe 1, du RGPD, c'est-à-dire d'une limitation aux droits et obligations de la personne concernée, laquelle ne peut se faire, en application du paragraphe 2 du même article, que dans des conditions spécifiques qui doivent être prévues par une disposition législative.

L'article 33 de l'avant-projet sera réexaminé en conséquence.

Article 34

Interrogée sur la date d'entrée en vigueur de l'avant-projet, laquelle n'est pas mentionnée à l'article 34 de l'avant-projet, la fonctionnaire déléguée a indiqué que l'intention de l'auteur de l'avant-projet était de faire entrer en vigueur les dispositions en projet le plus vite possible.

Il y a lieu en tout état de cause d'éviter que les dispositions en projet soient rétroactives.

Aangezien de adviesaanvraag ingediend is op basis van artikel 84, § 1, eerste lid, 2°, van de wetten ‘op de Raad van State’, gecoördineerd op 12 januari 1973, beperkt de afdeling Wetgeving overeenkomstig artikel 84, § 3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond van het voorontwerp,[‡] de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

Wat die drie punten betreft, geeft het voorontwerp aanleiding tot de volgende opmerkingen.

VOORAFGAAND VORMVEREISTE

Over het voorontwerp van wet dat aan de Raad van State voorgelegd is, is op 12 december 2018 advies nr. 009/2018 uitgebracht door het Controleorgaan op de politionele informatie.

Dat advies is aan de afdeling Wetgeving overgezonden in het Nederlands. Uit navraag bij de gemachtigde ambtenaar blijkt dat van dat advies geen Franse versie bestaat.

Het Controleorgaan op de politionele informatie (hierna te noemen: het “C.O.C.”) is bij artikel 71 van de wet van 30 juli 2018 ‘betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens’ opgericht bij de Kamer van volksvertegenwoordigers. Overeenkomstig artikel 59, § 1, tweede lid, van diezelfde wet dient het C.O.C. geraadpleegd te worden “bij het opstellen van een wet, een decreet of een ordonnantie, of een daarop gebaseerde reglementaire maatregel in verband met de verwerking (van persoonsgegevens)”.¹

In artikel 4, § 2, vierde lid, van de wet van 3 december 2017 ‘tot oprichting van de Gegevensbeschermingsautoriteit’ wordt bepaald dat “[d]e competenties, taken en bevoegdheden als toezichthoudende autoriteit voorzien door de Verordening 2016/79 (...) ten aanzien van de politiediensten in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie[dienst] gestructureerd op twee niveaus, uitgeoefend [worden] door het Controleorgaan op de politionele informatie bedoeld in artikel 44/6, § 1, van de wet van 5 augustus 1992 op het politieambt”. Voor de politiediensten dient ook verwezen te worden naar artikel 19 van de wet van 30 juli 2018.²

[‡] Aangezien het om een voorontwerp van wet gaat, wordt onder “rechtsgrond” de overeenstemming met de hogere normen verstaan.

¹ Die bepaling maakt deel uit van titel 2 van die wet (“De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door de bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid”).

² Dat artikel maakt deel uit van titel 1 van die wet (“De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens”).

internationale doorgifte van de gegevens, de bewaartermijnen van de gegevens, enz ... Telkens opnieuw verwees het Hof naar de controle door het Controleorgaan teneinde de (grond)wettelijkheid van deze bepalingen te rechtvaardigen.

De belangrijke rol die het Controleorgaan in het huidige systeem van politionele informatiehuishouding speelt en zelfs meer algemeen in de hele veiligheidsarchitectuur werd tot slot zeer recentelijk in de verf gezet door de parlementaire onderzoekscommissie 'belast met het onderzoek naar de omstandigheden die hebben geleid tot de terroristische aanslagen van 22 maart 2016 in de luchthaven Brussel-Nationaal en in het metrostation Maalbeek te Brussel, met inbegrip van de evolutie en de aanpak van de strijd tegen het radicalisme en de terroristische dreiging' (hierna 'POC Aanslagen') en meer bepaald in zijn 3^e tussentijds verslag over het onderdeel veiligheidsarchitectuur (*Parl. St.*, Kamer, 2016-2017, n^o 1752/008). Het thema van de (politionele) informatiehuishouding stond mede centraal in de werkzaamheden van de POC (zie voornamelijk het hoofdstuk IV, 'De informatiehuishouding'). (...)''⁴

Aangezien het overeenkomstig artikel 59, § 1, tweede lid, van de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens' de bedoeling is dat de adviezen van het C.O.C., zoals advies nr. 009/2018 van 12 december 2018, uitgebracht worden "bij het opstellen van [onder meer] een wet" en het belang van de betrokkenheid van het C.O.C. uitdrukkelijk onderstreept is, zowel door het Grondwettelijk Hof, in uitspraken over geschillen betreffende de fundamentele rechten en vrijheden, als in de memorie van toelichting van het ontwerp dat tot de wet van 30 juli 2018 geleid heeft, is het ondenkbaar dat het advies niet zowel in het Nederlands als in het Frans uitgebracht zou worden.⁵

Daarenboven is de tekst van het voorontwerp waarop de adviesaanvraag ingediend bij de afdeling Wetgeving van de Raad van State betrekking heeft niet gewijzigd naar aanleiding van het advies van het C.O.C. Teneinde te voorkomen dat de Raad van State, in het stadium van het voorontwerp dat voorafgaat aan dat waarin het ontwerp ter goedkeuring aan de Kamer van volksvertegenwoordigers voorgelegd wordt, advies zou uitbrengen over een niet-definitieve ontwerp tekst, verdient het aanbeveling om voorontwerpen van wet pas aan de Raad van State voor te leggen na afloop van de onderscheiden stadia van de administratieve voorbereiding van het voorontwerp.

Het zou overigens een goede zaak zijn als in de memorie van toelichting verduidelijkingen zouden staan over de wijze waarop in het ontwerp rekening gehouden is met het advies van het C.O.C.

⁴ *Parl.St.* Kamer 2017-18, nr. 54-3126/001, 115 tot 118.

⁵ Er wordt aan herinnerd dat het C.O.C. krachtens artikel 231, § 1, van de wet van 30 juli 2018, aldus georganiseerd is dat het tweetalig karakter ervan gegarandeerd is.

B. Beginnelsen inzake het recht op eerbiediging van het privéleven

In advies 63.192/2, dat de afdeling Wetgeving op 19 april 2018 gegeven heeft over een voorontwerp dat geleid heeft tot de wet van 30 juli 2018, is op het volgende gewezen:

“1. Zoals het Grondwettelijk Hof recent nog opgemerkt heeft⁷ in verband met het recht op eerbiediging van het privéleven dat gewaarborgd wordt door artikel 22 van de Grondwet, gelezen in samenhang met artikel 8 van het Europees Verdrag voor de rechten van de mens, artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten en de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, is de draagwijdte van artikel 8 EVRM analoog aan die van de voormelde grondwettelijke bepaling, zodat de waarborgen die deze beide bepalingen bieden een onlosmakelijk geheel vormen.

De artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie hebben, wat de verwerking van persoonsgegevens in het kader van de uitvoering van het Unierecht betreft, een draagwijdte die analoog is aan die van artikel 8 van het Europees Verdrag voor de rechten van de mens en aan die van artikel 22 van de Grondwet. Hetzelfde geldt voor artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten.

Het recht op eerbiediging van het privéleven, zoals gewaarborgd in de voormelde grondwets- en verdragsbepalingen, heeft voornamelijk tot doel de personen te beschermen tegen inmengingen in hun privéleven. Dat recht heeft een ruime draagwijdte en omvat onder meer de bescherming van persoonsgegevens en van persoonlijke informatie

In dat verband en wat de toepassingsgebieden buiten de Europese Unie betreft, wordt in Verdrag nr. 108 van de Raad van Europa van 28 januari 1981 “tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens”, dat bindend is voor de Belgische Staat, eveneens bepaald dat de Belgische Staat een reeks minimale waarborgen moet bieden.

2.1. Dat recht is evenwel niet absoluut. Het sluit overheidsinmenging in het recht op eerbiediging van het privéleven niet uit, maar het is vereist dat zij toegestaan wordt door een voldoende precieze wettelijke bepaling, dat zij beantwoordt aan een dwingende maatschappelijke behoefte in een democratische samenleving en dat zij evenredig is met de daarmee nagestreefde wettige doelstelling. Die bepalingen houden voor de overheid bovendien de positieve verplichting in om maatregelen te nemen die een daadwerkelijke eerbiediging van het privéleven verzekeren, zelfs in de sfeer van de onderlinge verhoudingen tussen individuen.

2.2. Doordat artikel 22 van de Grondwet aan de bevoegde wetgever de bevoegdheid voorbehoudt om vast te stellen in welke gevallen en onder welke voorwaarden afbreuk kan worden gedaan aan het recht op eerbiediging van het privéleven, waarborgt het aan elke burger dat geen enkele inmenging in dat recht kan plaatsvinden dan krachtens regels die zijn aangenomen door een democratisch verkozen beraadslagende vergadering. Een delegatie aan een andere macht is evenwel niet in strijd met het wettelijkheidsbeginsel voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de essentiële elementen voorafgaandelijk door de wetgever vastgesteld zijn.

2.3. Naast het formele wettelijkheidsvereiste legt artikel 22 van de Grondwet eveneens de verplichting op dat de inmenging in het recht op eerbiediging van het privéleven in

⁷ Voetnoot 2 van het geciteerde advies: GwH 14 juli 2016, nr. 108/2016, B.7 tot B.13; 15 maart 2018, nr. 29/2018, B.9 tot B.15.

regeling en het al dan niet voorhanden zijn van waarborgen ter voorkoming van foutief gebruik en misbruik van de verwerkte persoonsgegevens door de overheidsdiensten.

3. *In casu* houdt het recht op eerbiediging van het privéleven verband met de kern zelf van het voorontwerp dat aan de afdeling Wetgeving voorgelegd is. Het voorontwerp is dan ook onderzocht in het licht van de beginselen waaraan zonet herinnerd is.”

Dit voorontwerp dient eveneens in dat kader onderzocht te worden, rekening houdend met de lering van arrest nr. 108/2016 van het Grondwettelijk Hof van 14 juli 2016.⁹

BIJZONDERE OPMERKINGEN

DISPOSITIEF

Artikel 1

1. In artikel 1 van het voorontwerp staat dat “[d]eze wet (...) een aangelegenheid [regelt] als bedoeld in artikel 78 van de Grondwet”.

Het gaat evenwel om artikel 74 van de Grondwet.

Artikel 1 van het voorontwerp moet in die zin herzien worden.

2. Het voorontwerp moet aangevuld worden met een nieuwe bepaling die, overeenkomstig artikel 63, lid 1, tweede alinea, van die richtlijn vermeldt dat richtlijn 2016/680 wordt omgezet.

Artikel 2

In de Franse tekst van artikel 2, 1°, van het voorontwerp zijn het de woorden “*article 36ter de la loi du 8 décembre 1992 relative à la protection de la vie privée à l’égard du traitement des données à caractère personnel*” die vervangen moeten worden door de woorden “*article 71 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel*”.

Artikel 4

1. Aangezien in het ontworpen artikel 44/1, § 2, eerste lid, van de wet van 30 juli 2018 het begrip “gevoelige” gegevens gebruikt wordt, dient in het voorontwerp een bepaling ingevoegd te worden tot aanvulling van artikel 3 van de wet van 5 augustus 1992, in welke bepaling dat begrip “gevoelige gegevens” gedefinieerd wordt, waarbij artikel 10 van

⁹ Zie bijvoorbeeld overweging B.99.3.4 van dat arrest, in verband met artikel 44/1/9, § 2, van de wet op het politieambt (zie eveneens, wat dit punt betreft, opmerking nr. 15 van advies nr. 009/2018 dat het C.O.C. op 12 december 2018 uitgebracht heeft).

avec un haut degré de précision, ce que les Ministres devront opérationnaliser dans des directives.”

In advies 62.006/2, op 9 oktober 2017 gegeven over een voorontwerp dat geleid heeft tot 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, en tot wijziging van de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera’s, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en van de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid’, heeft de afdeling Wetgeving de gelegenheid gehad op het volgende te wijzen:

“In de bepaling onder 2° worden de ministers van Binnenlandse Zaken en van Justitie bij het ontworpen artikel 44/4, § 4, van de wet ‘op het politieambt’ gemachtigd om ‘bij gemeenschappelijke richtlijn de toereikende, terzake dienende en niet overmatige maatregelen [te bepalen] met betrekking tot de koppeling of correlatie van de technische gegevensbanken’ met andere gegevensbanken.

Er wordt aan herinnerd dat de bevoegdheden van verordenende aard die met betrekking tot die aangelegenheden aan de uitvoerende macht verleend worden, aan de Koning, en niet aan de ministers van Binnenlandse Zaken en van Justitie dienen opgedragen te worden.¹² (...)”.

In het voornoemde advies 63.192/2 heeft de afdeling Wetgeving ook het volgende opgemerkt:

“In artikel 46, § 4, vierde lid, en § 5, vierde lid, wordt bepaald dat de categorieën van contextuele informatie die door de bevoegde toezichthoudende autoriteit aan de betrokkene kunnen worden medegedeeld, bij ‘richtlijn’ bepaald worden door de bevoegde ministers nadat daarover het advies van de bevoegde toezichthoudende autoriteit ingewonnen is.

Dat het recht op de eerbiediging van het privéleven in beginsel bij wet geregeld moet worden, neemt weliswaar niet weg dat delegatie kan worden verleend aan een ander bevoegdheidsniveau, maar een dergelijke delegatie is enkel aanvaardbaar op voorwaarde dat deze voldoende nauwkeurig omschreven wordt en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de belangrijkste onderdelen op voorhand vastgesteld zijn door de wetgever.

A fortiori is het niet denkbaar dat de nadere regels met betrekking tot de waarborgen waarin voorzien wordt teneinde een kader te creëren voor de beperking van het recht op het privéleven die het gevolg is van de verwerking van persoonsgegevens, vastgesteld worden in een tekst die geenszins bindend is en bijgevolg ook niet beantwoordt aan de vereisten van voorzienbaarheid en rechtszekerheid.

Overigens staan de artikelen 33 en 108 van de Grondwet eraan in de weg dat de wetgever bepaalde uitvoeringstaken rechtstreeks aan een minister opdraagt. Het staat immers aan de uitvoerende macht om de werkwijze en de organisatie van haar diensten te regelen. De wet moet de Koning machtigen om de verschillende taken uit te voeren die worden genoemd. De Koning kan deze taken dan eventueel zelf delegeren.”

¹² Voetnoot 17 van het geciteerde advies: Zie advies 58.729/AV, op 26 januari 2016 gegeven over een voorontwerp dat ontstaan heeft gegeven aan de wet van 27 april 2016 ‘inzake aanvullende maatregelen ter bestrijding van terrorisme’ (*Parl.St.* Kamer 2015-16, nr. 1727/1, 127).

wijzigen, maar wel artikel 44/9, § 1, 2°, zodat de termijn vijf jaar zou bedragen, onder meer omdat bijvoorbeeld een stadionverbod zo lang kan duren.¹³

De steller van het voorontwerp dient het ontwerp dienovereenkomstig te herzien.

Artikel 14

1. In punt 12 van zijn advies 009/2018 van 12 december 2018 dringt het C.O.C. erop aan dat de oprichting van de bijzondere gegevensbanken mogelijk zou zijn “in specifieke omstandigheden” in plaats van “in uitzonderlijke omstandigheden”.¹⁴

Artikel 44/11/3, § 1, eerste lid, van het voorontwerp moet in die zin worden herzien.

2. Artikel 14 van het voorontwerp handelt over de oprichting of de wijziging van bijzondere gegevensbanken. Artikel 31 heeft dan weer betrekking op het register van de verwerkingsactiviteiten (ontworpen artikel 145 van de wet van 7 december 1998).

Het ontworpen artikel 44/11/3, § 3, van de wet van 5 augustus 1992 is als volgt gesteld:

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

Het Controleorgaan wordt, via het register van de verwerkingen van de politiediensten bedoeld in artikel 145 van de wet van 7 december 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.”

Op de vraag waarom niet voorgeschreven wordt dat de bijzondere gegevensbanken na advies van het Controleorgaan worden opgericht, maar enkel bepaald wordt dat het Controleorgaan “via het register (...) actief op de hoogte [wordt] gebracht” heeft de gemachtigde ambtenaar de volgende toelichtingen gegeven:

“Pour ce qui concerne les déclarations préalables des banques de données particulières au COC. Le COC indique lui-même dans son avis qu’il pourrait rendre un avis sur la base de l’accès direct qui lui serait fourni dans le registre des traitements et de la fonction alarme (il sera activement prévenu lorsqu’une nouvelle banque de données sera déclarée dans via ce registre). Il déclare lui-même que beaucoup de banques de données particulières sont en fait non sensibles. Dès lors obtenir un aval via un envoi séparé de ce registre ne représente pas beaucoup de plus-value. Rien n’empêche bien entendu le COC d’utiliser son pouvoir issu de l’article 59 de la loi cadre protection des données pour demander un accord sur certaines catégories de banques de données

¹³ Artikel 1, § 4, van het koninklijk besluit van 7 december 1999 ‘houdende de oprichting van een bestand van stadionverboden’.

¹⁴ “Het Controleorgaan, nadat het sedert 31 maart 2017 advies heeft verleend over zo’n 800 bijzondere gegevensbanken, pleit ervoor de woorden in ‘uitzonderlijke omstandigheden’ als voorwaarde voor het aanmaken van een bijzondere gegevensbank te schrappen”.

laatstgenoemde organen geen rechtstreekse toegang tot die informatie en persoonsgegevens hebben in zoverre artikel 44/11/3^{ter}, § 1, van dezelfde wet het enkel heeft over “het Orgaan”.¹⁶

Wat dat betreft, wordt verwezen naar artikel 47, lid 1, van richtlijn 2016/680, waarin het volgende wordt gesteld:

“Elke lidstaat voorziet erin bij wet dat elke toezichthoudende autoriteit effectieve onderzoeksbevoegdheden heeft”.

De ontworpen tekst moet dienovereenkomstig worden gewijzigd.

Artikel 20

Artikel 20 van het voorontwerp (ontworpen artikel 44/11/8^{bis} van de wet van 5 augustus 1992) maakt het mogelijk dat persoonsgegevens en informatie vervat in de A.N.G. worden meegedeeld aan het Coördinatieorgaan voor de dreigingsanalyse en aan de veiligheidsdiensten (lees: de inlichtingen- en veiligheidsdiensten).

Dienaangaande dient te worden opgemerkt dat, wanneer andere overheidsinstanties toegang wordt verleend, moet worden nagegaan of de doeleinden van de gegevensbanken wel in overeenstemming zijn met de wettelijke opdrachten van alle betreffende overheidsinstanties.¹⁷

De samenwerking tussen de politiediensten en de inlichtingen- en veiligheidsdiensten, waaronder de samenwerking betreffende de uitwisseling van gegevens, wordt trouwens reeds geregeld bij met name de artikelen 14, 16/4, 19 en 20 van de wet van 30 november 1998 ‘houdende regeling van de inlichtingen- en veiligheidsdiensten’.

Het is het een of het ander: ofwel moeten, indien de steller van het voorontwerp de bepalingen van de wet van 30 november 1998 een andere strekking wil geven, die bepalingen worden gewijzigd, ofwel moet, indien artikel 20 van het voorontwerp dezelfde strekking heeft als die bepalingen, artikel 20 worden weggelaten.

Artikel 27

Uit het ontworpen artikel 8^{sexies}, § 1, derde lid, van de wet van 7 december 1998 ‘tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus’ blijkt niet duidelijk of de covoorzitters die bij dat lid worden aangewezen, al dan niet behoren tot de veertien leden die krachtens het eerste lid van dezelfde bepaling het comité vormen.

De voorliggende bepaling moet verduidelijkt worden.

¹⁶ Zie ook artikel 44/11/3^{ter}, § 4, en artikel 44/11/3^{quater} van de wet van 30 juli 2018.

¹⁷ C. FORGET, “Titre 20 - La protection des données dans le secteur de la police et de la justice”, in C. de Terwangne en K. Rosier (ed.), *Le règlement général sur la protection des données (RGPD/GDPR)*, Brussel, Larcier, 2018, 879-880.

65.312/2avis du Conseil d'État/advies Raad van State31/31

Artikel 34 van het voorontwerp moet dienovereenkomstig worden herzien.

LE GREFFIER – DE GRIFFIER

LE PRÉSIDENT – DE VOORZITTER

Béatrice DRAPIER

Pierre VANDERNOOT



Advies COC-DPA n° 009/2018 van 12 december 2018

Betreft : advies betreffende het voorontwerp van wet betreffende het politionele informatiebeheer en tot wijziging van de wet op het politieambt en de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus

Het Controlegeaun op de politionele informatie (hierna "COC" ofwel "Controlegeaun").

Gelet op de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (BS, 5 september 2018, hierna afgekort als "GBW"), inzonderheid het artikel 71 en titel VII.

Gelet op de wet van 5 augustus 1992 op het politieambt (hierna afgekort "WPA"), inzonderheid 44/6.

Gelet op de aanvraag van de heer Jambon, Vice-Eerste Minister en Minister van Veiligheid en Binnenlandse Zaken van 19 november 2018 op grond van voormelde GBW betreffende een "voorontwerp van wet betreffende het politionele informatiebeheer en tot wijziging van de wet op het politieambt en de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus" (hierna afgekort als "het voorontwerp").

Gelet op het verslag van de heer Frank Schuermans, lid-raadsheer in het Controlegeaun.

Brengt op 12 december 2018 het volgend advies uit :

I. Voorafgaande opmerking nopens de bevoegdheid van het Controlegeaun

In het licht van, respectievelijk, de toepassing en omzetting van de Verordening 2016/679¹ en de Richtlijn 2016/680² heeft de wetgever de taken en opdrachten van het Controlegeaun grondig

¹ Verordening (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming of "AVG").

² Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing

voorontwerp heeft de ambitie dit algemene kader verder en in concreto te specificeren in de bestaande operationele en statutaire wetgeving betreffende de geïntegreerde politie. Er dient, aldus de memorie van toelichting, 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”*.

III. Onderzoek van het Ontwerp

3. Het Controleorgaan volgt in dit advies de chronologie van het voorontwerp maar gaat niet in op de louter technische aanpassingen. Deze technische aanpassingen hebben onder meer te maken met het nieuw juridisch kader van het Controleorgaan voorzien in artikel 71 en Titel VII van de GBW.

Opgemerkt dient wel dat niet in alle artikelen van de WPA de *“Commissie voor de Bescherming van de Persoonlijke Levensfeer”* vervangen wordt door het Controleorgaan of *“de bevoegde toezichthoudende autoriteit”* (vb. artikel 44/11/3bis §4 en §8, 44/11/3ter §2, 2^e lid en §3, 1^e en 2^e lid WPA). Het Controleorgaan verzoekt dat te doen. In de aanhef van het voorontwerp verzoekt het Controleorgaan te verwijzen naar haar huidig advies.

In het algemeen dient de steller van het ontwerp de Nederlandstalige versie van het ontwerp te herbekijken en te corrigeren. Het is duidelijk dat de originele tekst in het Frans werd ontworpen.

III.1. Wijzigingen aan de Wet van 5 augustus 1992 op het politieambt

4. Het eerste lid van het ontworpen artikel 44/1 §2 (artikel 4 voorontwerp) heeft weinig meerwaarde gezien de leden 2 en 4. Het maakt in wezen dubbel gebruik uit. Minstens dienen de woorden *“voornaamste doeleinde”* best te worden vervangen door, bijvoorbeeld, *“voor zover de verwerking van de in artikel 34 van de dezelfde wet bedoelde persoonsgegevens niet wordt beoogd”*. Ook een *“voornaamste”* doeleinde blijft immers een doeleinde. Ofwel is het een doeleinde, ofwel is het geen doeleinde. Maar, het valt inderdaad absoluut niet uit te sluiten dat deze gegevens *indirect* worden verwerkt. Het is daarom aangewezen in de memorie toe te lichten dat het een verwerking betreft die op zichzelf niet wordt beoogd, maar enkel element zijn bij de gegevensverzameling in het kader van hun de operationele politionele opdrachten (bijvoorbeeld wat de gerechtelijke politiefunctie betreft: gezondheidsgegevens bij een verkeersongeval; slagen en verwonden waarbij het motief mogelijks de geaardheid of afkomst van het slachtoffer is; bijvoorbeeld wat de bestuurlijke politiefunctie betreft: een lijst van groeperingen die de openbare orde verstoren zoals een groepering die uit salafisten bestaat die bekend staan voor hun aversie tegen de democratische waarden).

Het ontworpen artikel 44/1 §2 introduceert het begrip *“gevoelige gegevens”*. Het lijkt niet aangewezen dit begrip, dat weliswaar courant op het terrein wordt gebruikt, maar voor het overige in geen enkele regelgevende tekst wordt gedefinieerd, hier te gebruiken zonder het te definiëren. Noch in de AVG, noch in de richtlijn politie-justitie, noch in de GBW wordt dit begrip gebruikt. Het Controleorgaan adviseert derhalve het begrip te vermijden in het corpus zelf van het ontwerp, maar heeft er geen bezwaar tegen dat het wordt geduid in de toelichting. De correcte juridische term zijn de woorden *“bijzondere categorieën van persoonsgegevens”*.

Het COC verwelkomt de duidelijke aanduiding van de verwerkingsverantwoordelijke voor de drie soorten gegevensbanken daarin vermeld (te weten de ANG, de basisgegevensbanken en de bijzondere gegevensbanken). Het Controleorgaan wijst evenwel op de aanduiding van de "bevoegde overheden" in artikel 26, 7° GBW, met name *"de politiediensten in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie gestructureerd op twee niveaus"*. De beide voogdijministers dragen wel de (politieke) eindverantwoordelijkheid, maar de politiediensten dienen op grond van artikel 26, 7° GBW juncto artikel 2, 2°, WGP, indien al niet als (gezamenlijke) verwerkingsverantwoordelijke gezien te worden, dan toch minstens als operationele verwerkingsverantwoordelijke te worden aangeduid. Zij hebben immers de feitelijke invloed op de verwerking en bepalen in de feiten minstens mee de middelen die worden ingezet de beoogde doelen. Er kan ter inspiratie ook gekeken worden naar de voor de gemeenschappelijke gegevensbanken gebruikte termen "beheerder" en "operationeel verantwoordelijke" naast de eigenlijke verwerkingsverantwoordelijke. Een gelijkaardige constructie draagt de voorkeur van het COC weg voor de ANG en de basisgegevensbanken en zelfs voor de bijzondere gegevensbanken. Teneinde gelijkvormigheid tussen de diverse politionele gegevensbanken te bekomen opteert het COC ervoor de politiezone (voor de lokale politie) en de Minister van Binnenlandse Zaken en/of Justitie (voor de federale politie) aan te duiden als verwerkingsverantwoordelijke. De korpschef, commissaris-generaal, directeur-generaal en directeurs zijn dan de operationeel verantwoordelijke en beheerder. Op die wijze is er een juridische gelijkvormigheid in de aanduiding van de verwerkingsverantwoordelijk, operationeel verantwoordelijke en beheerder over alle politionele en gemeenschappelijke gegevensbanken heen.

De 2^e paragraaf voorziet voor alle in artikel 44/2 vermelde gegevensbanken (te weten de ANG, de basisgegevensbanken, de bijzondere gegevensbanken, de gemeenschappelijke gegevensbanken en de technische gegevensbanken) dat de beide Ministers bij richtlijn – het COC had haar graag zien staan "bij dwingende richtlijn" – de maatregelen vastleggen inzake beheer en veiligheid, alsmede dat voor elke verwerking in voormelde gegevensbanken logbestanden worden aangemaakt voor de meest essentiële bewerkingen. Het is vooreerst niet aangewezen in het 3^e lid van §2 het huidige artikel 56 GBW te parafraseren/kopiëren; een eenvoudige verwijzing naar artikel 56 GBW volstaat.

Die logbestanden moeten vervolgens in staat zijn de informatie te genereren voorzien door het overbodige ontworpen 3^e lid van §2 wat het COC verwelkomt nu dit op dit ogenblik niet met dergelijk detail mogelijk is. Het betreft dus een ambitieuze doelstelling die ook zal moeten waar gemaakt worden en waar de verwerkingsverantwoordelijken zullen kunnen op aangesproken worden. Zo bijvoorbeeld is het vermelden van een beweegreden van een verwerking (bv. in de ANG) tot op heden nog geen verplichting waaraan niet kan ontsnapt worden. Op dit ogenblik betreft het een facultatieve mogelijkheid die niet steeds nagekomen wordt, noch belet niets een politieambtenaar een drogreden in te geven. Wat de logbestanden betreft beklemtoont het COC dat het, zoals de toelichting ook stelt, te allen tijde toegang ertoe moet hebben ook al is er een beperkte gebruikerscode voorzien op de informatie.

Ook de ontworpen §3 is nieuw waar het de Ministers van Binnenlandse Zaken en Justitie oplegt om, elk binnen het kader van zijn bevoegdheden, bij richtlijn, de toegangsregels voor de leden van de politiediensten tot de gegevensbanken bedoeld in artikel 44/2, §1 en §3 vast te leggen. De omzendbrief MFO 3, die al zeer lang hopeloos achterhaald is en ook niet werd aangepast aan de ingrijpende wijzigingen van het juridisch kader inzake informatiehuishouding aangebracht door de Wet van 2014¹⁰ vraagt met dit voorontwerp een nog veel dringender update waarbij ook dit aspect

¹⁰ 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.

Het begrip “bestuurlijke maatregel” wordt niet gedefinieerd in de WPA (zie de definities onder artikel 3¹¹). Wel wordt het begrip gebruikt in artikel 30 WPA (i.v.m. de bestuurlijke inbeslagname, waar het begrip evenwel duidelijk wordt gehanteerd in zijn enge betekenis van (bestuurlijke) politimaatregel genomen door een politieambtenaar). Belangrijker lijkt het gebruik in artikel 44/9 (m.b.t. de archivering van de gegevens van de ANG) waar wordt gesproken over “een maatregel op basis van een beslissing van een bevoegde bestuurlijke of gerechtelijke overheid” (cf. art. 44/9 §1, 2° lid, a) en §2, 4° lid, 1° streepje en 7° lid, 1° streepje), maar waar er moet van uitgegaan worden dat de wetgever het hier heeft over een maatregel genomen door een (bestuurlijke) politieoverheid in de zin van artikel 3, 2° WPA.

De toelichting maakt evenwel duidelijk dat men hier een nog ruimere categorie van beslissingen viseert maar het blijft enigszins vaag vermits er op niet exhaustieve wijze enkele voorbeelden worden gegeven in de toelichting. Een aantal van die voorbeelden zijn bovendien geen bestuurlijke maatregel maar een zuiver bestuurlijke sanctie waarvan trouwens ook in de toelichting een concreet voorbeeld wordt gegeven (met name de sancties voorzien in de GAS-wet van 24 juni 2013). Het is cruciaal dat het in de wet duidelijk is welke maatregelen en sancties van welke overheden in de ANG en basisgegevensbanken kunnen gevat worden. In die zin stelt het COC voor klaarheid te scheppen en het ten 7° aan te vullen met het woord “sanctie” en lichtjes te herformuleren zodat het wordt: “de gegevens betreffende personen die het voorwerp uitmaken van een bestuurlijke maatregel of bestuurlijke sanctie genomen door een bevoegde bestuurlijke overheid en waarop de politiediensten door of krachtens de wet toezicht moeten uitoefenen of de handhaving waarborgen”. Het is dan duidelijk dat het niet alleen gaat om beslissingen genomen door een bestuurlijke politieoverheid (burgemeester, gouverneur, Minister van Binnenlandse Zaken) maar door eender welk bestuur gaat dat een maatregel of een sanctie kan nemen waarvan het toezicht op de naleving of de handhaving, door of krachtens de wet, tot de opdrachten van de politie behoort.

De overige wijzigingen aan artikel 44/5 leiden niet tot specifieke opmerkingen.

10. Aan artikel 44/9 met betrekking tot de archivering en wissing van de gegevens in de ANG worden enkele wijzigingen aangebracht (in het politiejargon dikwijls aangeduid als “ventilering”). Er wordt voorzien dat de nieuwe categorie van bestuurlijke maatregelen (en sancties, cf. hoger) worden geventileerd na ten laatste 3 jaar. Dit is, in tegenstelling tot wat de toelichting vermeldt, geen louter “technische aanpassing”. Het COC neemt akte van de keuze voor de kortste termijn van 3 jaar die inderdaad een maximale termijn is. Het komt aan de steller van het ontwerp toe te beoordelen of de ventilering na 3 jaar in alle gevallen overeenstemt met de duur van de maatregel. Het COC heeft geen zicht op alle bestaande potentiële maatregelen waarop de politie toezicht dient te houden maar stelt wel vast dat de meest voorkomende een kortere looptijd dan 3 jaar hebben (sluiting instelling, schorsing uitbatingsvergunning, plaatsverbod, ...). Maar, dat is niet altijd het geval. Zo moet er vastgesteld worden dat de authentieke bron van de administratieve stadionverboden (voetbalwet) die zich bevindt bij de FOD Binnenlandse zaken een bewaartermijn voorziet van 5 jaar¹²vermits een (administratief) stadionverbod als sanctie tot maximaal vijf jaar kan opgelegd worden.

In de praktijk stelt het COC hoe dan ook vast dat, behoudens bij punctuele aanpassingen naar aanleiding van bv. een verzoek tot onrechtstreekse toegang, de in artikel 44/9 gehanteerde

¹¹ Het begrip “politiemaatregel” wordt wel gedefinieerd maar is duidelijk enger dan het begrip bestuurlijke maatregel. Een politimaatregel moet uitgaan van een overheid van bestuurlijke of gerechtelijke politie wat niet noodzakelijk het geval is bij een bestuurlijke maatregel die bv. kan uitgaan van een gewone administratie.

¹² Artikel 1 §4 van het KB van 7 december 1999 houdende de oprichting van een bestand van stadionverboden.

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, maar de vaststelling is dan wel dat in de WPA niets te lezen valt omtrent dergelijke *“verschillende noodzakelijkheids- en proportionaliteitscriteria”*, noch worden die in de praktijk toegepast, voor zover ze al zouden bestaan. In beginsel worden immers alle persoonsgegevens en informatie gearhiveerd zonder enige noodzakelijkheids- of proportionaliteitstoets. De GBW is in deze de omzetting van onder meer de artikelen 4 en 5 van de Richtlijn politie-justitie die het op zijn beurt heeft over een **periodieke evaluatie** van opslag van de gegevens, waarmee ook een systeem van geautomatiseerde archivering van alle gegevens na verloop van een vaste termijn van bewaring op gespannen voet staat. Het komt aan de steller van het ontwerp toe hierin klaarheid te scheppen.

11. In het ontworpen artikel 44/11/2 (artikel 13 voorontwerp) wordt in de 2^e paragraaf het huidige 1^e lid geschrapt dat stelt dat *“de persoonsgegevens en informatie die worden verwerkt in de basisgegevensbanken zijn, met uitzondering van de persoonsgegevens en informatie die betrekking hebben op het beheer van onderzoeken, slechts beschikbaar en rechtstreeks raadpleegbaar door de politiediensten die ze geregistreerd hebben of de politiediensten die ze, wegens hun wettelijke opdrachten, moeten coördineren”*. Daarmee wil de steller van het ontwerp de huidige, vanuit legistiek standpunt problematische, praktijk van koppeling van de basisgegevensbanken ISLP van verschillende lokale politiezones aan elkaar (cf. hoger het onderzoek INFOTHEEK van het COC) uit de wettelijke schemerzone halen. Het COC heeft daar zelf voor gepleit in zijn controleonderzoek nu de operationele meerwaarde van dergelijke koppelingen onbetwistbaar is, maar anderzijds ook grotere gevaren stelt op het vlak van privacy en gegevensbescherming, nu voormelde toepassing een typevoorbeeld is van gevallen waarin de politie met niet gevalideerde informatie zal werken en mogelijk ook bepaalde politionele handelingen zal stellen met al dan niet uitvoering van dwang of geweld. Vandaar de noodzaak om in die gevallen de nodige grendels en zekerheden in te bouwen waarop hoger werd gewezen (cf. randnummer 8).

12. In artikel 44/11/3 WPA dat de bijzondere gegevensbanken regelt (artikel 14 voorontwerp) wordt de eerste paragraaf vervangen en wordt vooral aangegeven welke categorieën van gegevens er kunnen in opgenomen worden. Het Controleorgaan, nadat het sedert 31 maart 2017 advies heeft verleend over zo'n 800 bijzondere gegevensbanken, pleit ervoor de woorden *“in uitzonderlijke omstandigheden”* als voorwaarde voor het aanmaken van een bijzondere gegevensbank te schrappen.

Vooreerst weet niemand juist, en al zeker de politie niet, wat moet verstaan worden onder *“uitzonderlijke omstandigheden”*. Het Controleorgaan heeft bij de aangifte van tientallen van bijzondere gegevensbanken al evenzeer geworsteld met deze notie temeer heel wat aangiften helemaal niets *“uitzonderlijks”* bleken te zijn, maar eenvoudigweg onderdeel van de reguliere politiewerking. M.a.w. zeer vele zogenaamde bijzondere gegevensbanken maken deel uit van wat als routineopdrachten en bevoegdheden van een politiedienst kunnen beschouwd worden binnen de normale uitoefening van de taken van bestuurlijke en gerechtelijke politie. Omdat evenwel het aangegeven databestand noch als onderdeel van een basisgegevensbank, noch als onderdeel van de ANG kan worden aanzien werden vele onder hen toch als een bijzondere gegevensbank beschouwd door het Controleorgaan, omdat men anders zou kunnen redeneren dat het bestand gewoonweg geen juridische basis zou hebben vermits de opsomming van de bestaande politionele gegevensbanken een limitatieve opsomming is. Voorbeelden zijn bijzondere gegevensbanken met de gegevens van transmigranten, of personen van wie er aanwijzingen van radicalisering zijn, of een databank met persoonsgegevens gelieerd aan schepen en hun eigenaars, of de databank *“Mercure”* voor het beheer van de gegevens uit een telefonie-onderzoek, of een databank van personen die in de zone wonen en

gezien en daaruit bleek reeds duidelijk dat de erin gevatte informatie te summier is om het Controleorgaan toe te laten met kennis van zaken een (eerste) evaluatie te doen (zonder m.a.w. ter plaatste in de databank te moeten gaan kijken).

13. In artikel 44/11/3ter §1 WPA dat een omschrijving bevat van de diensten/organen die een rechtstreekse toegang hebben tot de gemeenschappelijke gegevensbanken ontbreekt op heden die toegang voor zowel het COC als het Vast Comité I. Bij de beheerder van de databank, met name de federale politie, is er enige discussie nopens de vraag of er actueel een juridische basis is voor beide controle-instanties om een rechtstreekse toegang te hebben. Het is met name de federale politie die er zorg moet voor dragen op technisch vlak dat die toegang verleend wordt.

Voor het COC is die rechtsbasis glashelder vermits in §1, 1^e lid letterlijk sprake is van toegang voor “het orgaan” waarmee alleen maar het COC kan zijn bedoeld. Vreemd genoeg echter wordt het Comité I daarin niet vermeld wat kennelijk een vergissing is. Het is hoe dan ook het uitgelezen moment om klaarheid te scheppen en de rechtstreekse toegang uitdrukkelijk te voorzien voor zowel het COC als het Vast Comité I. Dat kan ofwel in dit artikel ofwel kan dat uitdrukkelijk voorzien worden in het ontworpen artikel 44/11/3quinquies/2 WPA. Dat beide controleorganen nood hebben aan dergelijke rechtstreekse toegang kan niet ernstig betwijfeld worden. Een gedegen controle is maar mogelijk indien de toezichthoudende autoriteit dezelfde toegang heeft als de basisdiensten. Zowel de AVG als de Richtlijn politie-justitie voorziet overigens dat de toezichthoudend autoriteit “*effectieve onderzoeksbevoegdheden*” moet hebben. Het COC heeft overigens al een rechtstreekse toegang tot de ANG. De voorkeur van het COC gaat duidelijk uit naar een specifieke uitdrukkelijke bepaling in het ontworpen artikel 44/11/3quinquies/2 WPA waar tussen het 1^e en 2^e lid (dat het 3^e lid zou worden) het volgende lid zou worden ingevoegd: “*op basis van de behoefte om te kennen, zijn alle of een gedeelte van de persoonsgegevens en informatie van de gemeenschappelijke gegevensbanken ten alle tijde rechtstreeks toegankelijk voor het Controleorgaan en het Vast Comité van toezicht op de inlichtingen – en veiligheidsdiensten. De beheerder draagt zorg voor de totstandkoming van voormelde rechtstreekse toegang*”.

In dat opzicht is ook het begin van voormeld artikel en met name de zinssnede “*Met eerbied voor de uitoefening van hun respectievelijke bevoegdheden*” niet erg helder. Beide toezichthoudende autoriteiten kunnen hun respectievelijke bevoegdheden (voor het COC opgenomen in de GBW en voor het Comité I opgenomen in de Wet van 18 juli 1991) uitoefenen bij de controle op de gemeenschappelijke gegevensbanken. Dat wordt dan ook best zo geformuleerd: “*De controle op de verwerking van de in de gegevensbanken bedoeld in artikel 44/2, §2 vervatte informatie en persoonsgegevens wordt, in overeenstemming met hun bevoegdheden opgenomen in respectievelijk de wet gegevensbescherming en de wet van 18 juli 1991 tot regeling van het toezicht op politie – en inlichtingendiensten en het Coördinatieorgaan voor de dreigingsanalyse verzekerd door het Controleorgaan en het Vast Comité van Toezicht op de inlichtingendiensten zoals bedoeld in artikel 28 van voormelde Wet van 18 juli 1991*”.

Voor de volledigheid wenst het Controleorgaan op te merken dat de verwijzingen naar “het Orgaan” in artikel 44/11/3ter §4 en artikel 44/11/3quater kennelijk op een vergissing berust. De verwijzing naar het Controleorgaan dient in deze bepalingen te worden geschrapt. Het Controleorgaan stelt tot slot nog vast dat het actuele artikel 44/11/3quinquies WPA door het ontwerp niet wordt gewijzigd hoewel ook daar, in zijn 2^e lid nog wordt gerefereerd naar de inmiddels opgeheven Wet Verwerking Persoonsgegevens van 8 december 1992. De steller van het ontwerp zal ook deze bepaling willen aanpassen aan het nieuwe vigerende wetgevend kader.

het COC geen idee van die modaliteiten heeft (betreft het ook een rechtstreekse toegang, enkel een bevraging of een wat meer gestructureerde punctuele mededeling?) is het niet bij machte een correcte inschatting te maken van voormelde gegevensstroom naar de politie. Ook de toelichting verschaft op dat punt niet meer duidelijkheid.

Op dit moment hebben de inlichtingendiensten reeds een juridische grondslag voor een rechtstreekse bevraging van de ANG en dit sedert april 2014 maar die wordt in de praktijk, om voor het COC onbekende redenen, niet toegepast. Dat wordt ook, zij het impliciet, erkend in de toelichting waar gesteld wordt dat de uitwisseling van informatie nu *"immers aan de hand van ad hoc-mechanismen via formele tussenpersonen ... of via de contacten die op gezette tijdstippen plaatsvinden tussen onderzoekers ... 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 systematisch overdracht van bepaalde documenten via e-mail ..., maar ook vaak op vraag van een onderzoeker van de inlichtingendiensten ..."* (p. 31). Het is dus onduidelijk of het bestaande systeem van rechtstreekse bevraging van de ANG via een *"hit no hit"*-functie voor de inlichtingendiensten onvoldoende zou zijn en zo ja waarom dat zo zou zijn. Voor alle duidelijkheid een rechtstreekse bevraging van de ANG laat reeds zeer veel toe. Het laat de inlichtingendiensten, op grond van artikel 44/11/4 §3 WPA, toe om een rechtstreekse toegang te hebben *"tot alle of een gedeelte van de volgende gegevens:*

- a) het bestaan van gegevens over een persoon met toepassing van de artikelen 44/5, § 1, eerste lid, 2° tot 6°, en § 3, 1° tot 9°;*
 - b) de door de politie weerhouden kwalificatie betreffende de feiten waarvoor de persoon geregistreerd werd;*
 - c) de noodzakelijke gegevens om meer informatie te bekomen vanwege de bevoegde overheid en*
 - d) de gegevens met betrekking tot de te nemen maatregelen voor de in punt a) bedoelde personen",*
- op grond waarvan dan verder contact kan opgenomen worden door de inlichtingendiensten met de betrokken politiedienst – of ambtenaren om nog meer detailinformatie te bekomen.

Nog vooraleer derhalve duidelijk of minstens aannemelijk wordt gemaakt dat de rechtstreekse bevraging de inlichtingendiensten niet zouden toelaten hun opdrachten naar behoren uit te voeren, noch waarom men kennelijk deze mogelijkheden in de praktijk niet benut, wordt de ANG **volledig** "opengezet" ten voordelen van de inlichtingendiensten door een rechtstreekse bevraging. Deze uitbreiding is, in tegenstelling tot wat de toelichting lijkt de stellen, wel degelijk zeer substantieel en plaats de inlichtingendiensten als uitvoerende organen op dezelfde hoogte als de bestuurlijke en gerechtelijke overheden en onafhankelijke toezichtsorganen. Voor het OCAD lijkt er minder bezwaar voorhanden omdat het OCAD geen inlichtingendienst is met operationele bevoegdheden. Een rechtstreekse bevraging laat de inlichtingendiensten alleszins toe kennis te nemen van alle voorgaande politionele en gerechtelijke antecedenen van een betrokkene, ook degenen die geen enkel uitstaans hebben (vb. loutere zedenzaken, gemeenrechtelijke valsheden, verkeersmisdrijven, gewone fiscale en sociale fraude, enz ...) met de bevoegdheden van de inlichtingendiensten en dit zonder dat er enige filter van toepassing is, wat niet het geval is bij de actueel geldende rechtstreeks bevraging. Het feit

Meer in het bijzonder wanneer het optreden van de overheid een geheim karakter vertoont, dient de wet voldoende waarborgen te bieden tegen willekeurige inmengingen in het recht op eerbiediging van het privéleven, namelijk door de beoordelingsbevoegdheid van de betrokken overheden op voldoende duidelijke wijze af te bakenen, enerzijds, en door te voorzien in procedures die een effectief jurisdictioneel toezicht toelaten, anderzijds (EHRM, grote kamer, 4 mei 2000, Rotaru t. Roemenië, § 55; 6 juni 2006, Segerstedt-Wiberg t. Zweden, § 76; 4 juli 2006, Lupsa t. Roemenië, § 34)".

16. De technische wijziging aan artikel 44/10/10 (artikel 22 voorontwerp) WPA is de gelegenheid voor het COC om te wijzen op de actueel zeer prangende problematiek van de mededeling van politionele persoonsgegevens aan instellingen voor wetenschappelijk onderzoek of onderzoekers van wetenschappelijke instellingen waaromtrent de rechtsonzekerheid zeer groot is. Hieromtrent werd het advies COC-CONTROLE-002-2018 van 23 oktober 2018 overgemaakt aan de steller van het ontwerp. Voormelde bepaling stelt dat een Koninklijk besluit, na advies van (in de toekomst) het Controleorgaan, zal bepalen aan welke instellingen of personen de persoonsgegevens die noodzakelijk zijn voor het vervullen van de hen door of krachtens een wet, een decreet of een ordonnantie toevertrouwde opdrachten van openbaar nut die aan wetenschappelijk onderzoek verbonden zijn, kunnen meegedeeld worden. Dat besluit moet tevens de nadere regels van deze mededeling bepalen.

Deze bepaling, die op 7 april 2014 in werking is getreden, werd tot op heden nooit uitgevoerd zodat, strikt genomen, aan onderzoekers van universiteiten of hoge scholen geen politionele gegevens kunnen overgemaakt worden wat evident majeure problemen voor het wetenschappelijk onderzoek en ook voor de politiediensten oplevert. Actueel kan men zich, voor zover de politionele gegevens zich ook op proces-verbaal bevinden en dus onderdeel uitmaken van een strafdossier, behelpen met punctuele toelatingen van het bevoegde openbaar ministerie. Indien dat echter niet het geval is, bijvoorbeeld gegevens over de patrouilles, interventieplaatsen en soorten interventies, enz ... stelt zich een heus juridisch probleem. Het COC werd hieromtrent reeds bevraagd bijvoorbeeld door de Universiteit Gent die binnen en op vraag van de politiezone Antwerpen een wetenschappelijk onderzoek wil doen naar de mogelijkheden en beperkingen van het zgn. "predictive policing" concept, waarvoor een hele schare aan politionele data, waaronder persoonsgegevens noodzakelijk zijn. Bij gebrek aan uitvoeringsbesluit balanceren dergelijk onderzoeken op een slappe koord of weigert de politie die gegevens te verstrekken nu het niet zeker is dat er een afdoende juridische grondslag voorhanden is.

Het ontbreken van een uitvoeringsbesluit is des te opmerkelijker vermits, voor andere veiligheidsdiensten, zoals bijvoorbeeld de inlichtingendiensten of het OCAD, de GBW nu net wél in een specifieke regeling heeft voorzien voor het gebruik van de door deze instellingen verwerkte gegevens voor wetenschappelijke doeleinden. Er moet inderdaad verwezen worden naar hoofdstuk X ("*verwerking van persoonsgegevens voor historische, wetenschappelijke of statistische doeleinden*") van ondertitel 1 (de artikelen 99 tot en met 104), van ondertitel 3 (de artikelen 132 tot en met 137) en van ondertitel 4 (de artikelen 162 tot en met artikel 167) van titel III van de GBW die dienaangaande een eigen regeling hebben voorzien voor dergelijke mededeling van persoonsgegevens. Het legt de verantwoordelijkheid voor deze mededeling bij de respectievelijke diensten als verwerkingsverantwoordelijke. Het is evident niet logisch dat het actueel juridisch kader deze mogelijkheden niet voorziet voor politiedata waaraan door de band genomen bij de wetenschappelijke wereld veel meer vraag is.

Een andere optie is desgevallend het COC een bindend advies te laten geven waarbij het aan het COC zou toekomen de wettelijkheid (finaliteit, gegevensbeperking, informatieveiligheid, enz ...) en proportionaliteit van de mededeling van de politionele gegevenstransfer naar de onderzoeker(s) te beoordelen. Dit zou meteen in het verlengde liggen van en is gelijkaardig aan de bevoegdheid van het COC voorzien in het hoger besproken artikel 44/11/9 §2 WPA. In dat geval is er geen Koninklijk besluit meer nodig.

III.2. Wijzigingen aan de Wet op de Geïntegreerde politie van 7 december 1998

entiteiten van de federale politie. Uit de toelichting lijkt impliciet te kunnen worden afgeleid dat het verplichtend karakter de bedoeling is. Het lijkt het COC verkieselijk de wettelijke verplichting meteen in artikel 145 in te schrijven.

Ook hier verzoekt het COC in het ontworpen artikel 145 het advies van het Controleorgaan verplicht te maken bij de opmaak van het aldaar bedoelde uitvoeringsbesluit die de vorm en de modaliteiten van het register zal vastleggen.

20. Het ontworpen artikel 146 is een toepassing van artikel 9.2 van de Richtlijn politie-justitie. De bepaling is wel zeer algemeen. Het Controleorgaan stelt voor te verwijzen naar artikel 29 GBW: *"In overeenstemming met de voorwaarden van artikel 29 GBW delen de verwerkingsverantwoordelijken ..."*

21. Het ontworpen artikel 147 (artikel 33 voorontwerp) voorziet ook voor verzoeken tot inzage in AVG-materiaal, waarbij sprake is van een verwerking van gegevens die aanvankelijk door de politie verwerkt werd in toepassing van titel 2 GBW, in een onrechtstreekse toegang bij de uitoefening van zijn rechten via het Controleorgaan. Dit artikel sluit aan bij artikel 14 §6 GBW dat evenzeer het COC een verantwoordelijkheid heeft bij verzoeken tot uitoefening van de betrokkene van zijn rechten bij een overheid die onder titel 1 GBW/AVG valt en het betrekking heeft op informatie die oorspronkelijk door de politiediensten (in hun operationele opdrachten) verwerkt werden. Het 2^e lid van de 1^e paragraaf lijkt overbodig en dubbel gebruik uit te maken met artikel 14 §2 GBW.

Er wordt in casu niet gespecificeerd welke informatie het COC in dat geval kan/mag meedelen aan betrokkene. In voormeld artikel 14 §6, 2^e lid GBW wordt gesteld dat wanneer de GBA gevat werd door de betrokkene, na ontvangst van het antwoord van het Controleorgaan, de GBA de betrokkene informeert *"volgens de vastgelegde wettelijke nadere regels"*. Welke die laatste zijn wordt niet verduidelijkt. Hoe dan ook, bij gebrek aan nadere omschrijving zal het tot de verantwoordelijkheid van het COC behoren te bepalen welke informatie kan gegeven worden. Dat is overigens ook de voorkeur van het Controleorgaan. De enkele melding dat *"de nodige verificaties werden verricht"*, zoals voorzien onder titel 2 (artikel 42 GBW) stuit zeer vaak op volstrekt onbegrip bij de betrokkene.

Meer algemeen moet er overigens worden opgemerkt dat artikel 41 GBW niet rechtstreeks een systeem van onrechtstreekse toegang invoert hoewel dat kennelijk links en rechts op het terrein als overtuiging leeft. Voormeld artikel bepaalt immers: *"de wet, het decreet of ordonnantie bepalen dat de rechten van de betrokkene door de bevoegde toezichthoudende autoriteit worden uitgeoefend"*. Hoewel deze bepaling in die zin zou kunnen gelezen worden dat met "wet" ook de GBW zelf wordt bedoeld, lijkt dat niet het opzet van de wetgever te zijn geweest. In de memorie van toelichting bij de GBW wordt het opzet van artikel 41 GBW immers als volgt verantwoord: *"Het is de bedoeling om het systeem van de onrechtstreekse toegang als mogelijkheid te behouden voor de overheden die dat wensen. Er wordt ook bepaald dat wanneer de onrechtstreekse toegang wordt toegepast, het verzoek wordt ingediend bij de bevoegde toezichthoudende autoriteit"*.¹⁷ Dat artikel 42 bepaalt dat het verzoek aan het COC moet worden gericht is de loutere implementatie van artikel 17, 1^e lid van de Richtlijn politie-justitie. Er dient dus in de WPA best een einde gemaakt te worden aan deze onduidelijkheid.

22. Het Controleorgaan heeft er tot slot volste begrip voor dat de ambitieuze bepalingen met betrekking tot de loggings niet allemaal onmiddellijk kunnen in werking treden. Het betreft de loggings voor wat betreft de verwerkingen in de ANG, in de archieven van de ANG, in de basisgegevensbanken en in de bijzondere gegevensbanken. De verwijzing in het artikel 34 van het voorontwerp naar artikel 279 GBW is wellicht een vergissing; men bedoelt ongetwijfeld artikel 284 GBW. Voor wat evenwel de verwerkingen in de ANG betreft ziet het Controleorgaan geen enkele goede reden om de bewaring van

¹⁷ Parl. St. Kamer 2017-2018, 54-3126/001, 84. Eigen markering.

**Avis COC-DPA-A n° 009/2018 du 12 décembre 2018**

DA180009

Objet : avis concernant l'avant-projet de loi relatif à la gestion de l'information policière et modifiant la loi sur la fonction de police et la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux

L'Organe de contrôle de l'information policière (ci-après "le COC" ou "l'Organe de contrôle").

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (M.B. du 5 septembre 2018, ci-après la "LPD"), en particulier l'article 71 et le titre VII.

Vu la loi du 5 août 1992 *sur la fonction de police* (ci-après la "LFP"), en particulier l'article 44/6.

Vu la demande du 19 novembre 2018 de Monsieur Jambon, Vice-premier ministre et Ministre de la Sécurité et de l'Intérieur, en vertu de la LPD précitée, concernant un "*avant-projet de loi relatif à la gestion de l'information policière et modifiant la loi sur la fonction de police et la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux*" (ci-après "l'avant-projet").

Vu le rapport de Monsieur Frank Schuermans, membre-conseiller de l'Organe de contrôle.

Émet, le 12 décembre 2018, l'avis suivant :

I. Remarque préalable concernant la compétence de l'Organe de contrôle

À la lumière respectivement de l'application et de la transposition du Règlement 2016/679¹ et de la Directive 2016/680², le législateur a profondément modifié les tâches et les missions de l'Organe de contrôle. L'article 4, § 2, troisième alinéa de la loi organique du 3 décembre 2017 *portant création de l'Autorité de protection des données*³ dispose que pour les services de police au sens de l'article 2, 2° de la loi du 7 décembre 1998 *organisant un service de police intégré, structuré à deux niveaux*⁴, les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle.

Cela signifie notamment que l'Organe de contrôle est également compétent lorsque des services de police traitent des données à caractère personnel qui ne relèvent pas des missions de police administrative et judiciaire, par exemple dans le cadre de finalités socio-économiques ou de traitements de ressources humaines.

L'Organe de contrôle doit être consulté dans le cadre de la préparation d'une législation ou d'une mesure réglementaire liée au traitement de données à caractère personnel par les services de police de la police intégrée (voir l'article 236, § 2 de la LPD⁵, l'article 36.4 du RGPD et l'article 28.2 de la Directive Police et Justice). Dans ce cadre, l'Organe de contrôle a pour mission d'examiner si l'activité de traitement envisagée par les services de police est conforme aux dispositions des Titres 1^{er} (pour les traitements non opérationnels) et 2 (pour les traitements opérationnels) de la LTD⁶.

En ce qui concerne en particulier les activités de traitement dans le cadre des missions de police administrative et/ou de police judiciaire, l'Organe de contrôle émet un avis, soit d'initiative, soit à la demande du gouvernement ou de la Chambre des représentants, d'une autorité administrative ou judiciaire ou d'un service de police concernant toute question relative à la gestion de l'information policière, telle que régie dans la section 12 du chapitre 4 de la loi *sur la fonction de police*⁷.

En outre, à l'égard des services de police, de l'Inspection générale de la police fédérale et de la police locale telle que visée dans la loi du 15 mai 2007 sur l'Inspection générale et de l'Unité d'information des passagers visée au chapitre 7 de la loi du 25 décembre 2016, l'Organe de contrôle est également chargé du contrôle de l'application du Titre 2 de la LPD, du traitement de données à caractère personnel tel que visé aux articles 44/1 à 44/11/13 de la loi *sur la fonction de police*⁸ et de toute autre mission qui lui est confiée par ou en vertu d'autres lois.⁹

II. Objet de la demande

1. L'avant-projet a pour but d'adapter les règles relatives à la gestion de données à caractère personnel et d'informations par les services de police au nouveau cadre juridique européen et national en matière de protection des données. Il s'agit bien entendu du RGPD, de la Directive Police et Justice

¹ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (Règlement général sur la protection des données ou RGPD).

² Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données et abrogeant la décision-cadre 2008/977/JAI du Conseil* (ci-après la "Directive Police et Justice").

³ En abrégé ci-après : "loi LPD".

⁴ En abrégé ci-après : LPI.

⁵ En abrégé ci-après : LPD.

⁶ Article 59, § 1, 2°, deuxième alinéa de la LPD.

⁷ Article 236, § 1 de la LPD.

⁸ En abrégé ci-après : LFP.

⁹ Article 236, § 3 de la LPD.

2016/680, de la LPD et de la loi APD. Le Titre 2 de la LPD fixe le cadre général. L'avant-projet a l'ambition de spécifier plus avant ce cadre général *in concreto* dans la législation opérationnelle et statutaire existante relative à la police intégrée. D'après l'Exposé des motifs, il faut assurer *"un degré élevé à la fois de protection et de sécurisation des données à caractère personnel et de leur traitement. 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."*

III. Examen du projet

3. Dans le présent avis, l'Organe de contrôle suit la chronologie de l'avant-projet mais ne se penche pas sur les adaptations purement techniques. Ces adaptations techniques concernent notamment le nouveau cadre juridique de l'Organe de contrôle prévu à l'article 71 et au Titre VII de la LPD.

Il convient toutefois de remarquer que dans la LFP, les termes *"Commission de la protection de la vie privée"* n'ont pas été remplacés dans tous les articles par l'Organe de contrôle ou *"l'autorité de contrôle compétente"* (par exemple à l'article 44/11/3bis, § 4 et § 8, à l'article 44/11/3ter, § 2, 2^e alinéa et § 3, 1^e et 2^e alinéa de la LFP). L'Organe de contrôle demande de le faire. Dans l'en-tête de l'avant-projet, l'Organe de contrôle demande de renvoyer au présent avis.

De manière générale, l'auteur du projet doit revoir et corriger la version néerlandaise du projet. Il est évident que le texte original a été rédigé en français.

III.1. Modifications de la loi du 5 août 1992 sur la fonction de police

4. Le premier alinéa du projet d'article 44/1, § 2 (article 4 de l'avant-projet) présente peu de plus-value vu les alinéas 2 et 4. En soi, il fait double emploi. Les termes *"objet principal"* devraient de préférence au moins être remplacés, par exemple par *"pour autant que l'on ne vise pas le traitement des données à caractère personnel visées à l'article 34 de la même loi"*. Même une finalité *"principale"* reste en effet une finalité. Soit c'est une finalité, soit ce n'en est pas une. Mais on ne peut pas absolument exclure que ces données soient traitées *indirectement*. Il est dès lors recommandé d'expliquer dans l'Exposé des motifs qu'il s'agit d'un traitement qui n'est pas intrinsèquement visé, mais qu'il s'agit d'un élément dans la collecte de données dans le cadre de leurs missions policières opérationnelles (en ce qui concerne par exemple la fonction de police judiciaire : des données de santé lors d'un accident de la route ; des coups et blessures dont le motif est probablement la nature ou les origines de la victime ; en ce qui concerne par exemple la fonction de police administrative : une liste de groupements qui perturbent l'ordre public comme un groupement composé de salafistes qui sont connus pour leur aversion envers les valeurs démocratiques).

Le projet d'article 44/1, § 2 introduit la notion de *"données sensibles"*. Il ne semble pas recommandé d'utiliser ici cette notion sans la définir. Celle-ci est certes utilisée couramment sur le terrain mais elle n'est pour le reste définie dans aucun texte réglementaire. Ni le RGPD, ni la Directive Police et Justice, ni la LPD n'utilisent cette notion. L'Organe de contrôle recommande dès lors d'éviter cette notion dans le corps du projet, mais il n'a pas d'objection à ce qu'on l'explique dans l'Exposé des motifs. Les termes juridiques corrects sont *"catégories particulières de données à caractère personnel"*.

5. Dans le deuxième alinéa du projet d'article 44/1, § 2, l'Organe de contrôle recommande d'ajouter, entre les termes *"en complément"* et le terme *"d'autres"*, les termes *"et en appui"* afin que la phrase devienne : *"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 traitées en complément et/ou en appui d'autres catégories de données visées à l'article 44/5."* En général, ces données seront en effet plutôt en appui dans le travail policier quotidien, à des fins par exemple de preuve dans le cadre des missions de police judiciaire. Une même remarque s'applique au 3^e alinéa qui traite de données biométriques et au 4^e alinéa qui traite des données de santé (voir également la remarque au point 4).

6. Au 4^e alinéa, les possibilités pour les services de police de traiter des données relatives à la santé, outre le caractère complémentaire (et d'appui, cf. point 5) du traitement, sont encore réduites par les termes *"et 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."* L'auteur du projet doit réfléchir à la question de savoir si tous les traitements de données relatives à la santé réalisés couramment dans la pratique par la police sont ainsi couverts. Le dernier segment (*"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"*) ne requiert aucune précision, mais vise un cas d'application particulier et vise la protection de tiers (qu'ils soient ou non membres du personnel des services de police). Le premier segment (*"dans le but de comprendre le contexte lié à la personne concernée"*) est par contre sujet à interprétation. Il est ainsi évident que la police doit pouvoir traiter des données relatives à la santé dans le cadre de la constatation de toutes sortes d'infractions contre l'ordre des familles et contre la moralité publique (Livre II, Titre VII du Code pénal), tant concernant un suspect qu'une victime. Il ne s'agit pas tant du *"contexte lié à la personne concernée"* mais simplement par exemple de son état de santé (porteur d'une maladie, patient cardiaque, historique de problèmes psychiatriques, etc.). L'Organe de contrôle estime à cet égard que les termes employés sont dès lors ambigus (il semble plutôt s'agir de circonstances externes), avec toutes les conséquences qui en découlent sur la régularité des futurs actes policiers d'information ou d'instruction, ou de manière plus générale sur la régularité de la procédure. Il semble préférable d'exclure les discussions à ce niveau et il incombe dès lors à l'auteur du projet de clarifier les choses. Cette clarté peut consister simplement à faire référence à la nécessité de traiter des données relatives à la santé pour l'exercice de leurs missions de police administrative ou judiciaire et la protection de la santé de tiers.

7. L'article 44/3 (article 6 de l'avant-projet) est adapté afin de remplacer la fonction de conseiller en sécurité et en protection de la vie privée par celle de "Data Protection Officer" (DPO) ou délégué à la protection des données et doit être lu conjointement avec le projet d'article 144 de la loi relative à la police intégrée du 7 décembre 1998 (ci-après "LPI"). L'Organe de contrôle n'a pas de remarque particulière à formuler à cet égard étant donné que tout cela est conforme au nouveau cadre de protection des données.

8. L'article 44/4 de la LFP est remplacé intégralement (article 7 de l'avant-projet).

Le COC salue la désignation claire du responsable du traitement pour les trois types de banques de données (à savoir la BNG, les banques de données de base et les banques de données particulières). L'Organe de contrôle souligne toutefois la désignation des "autorités compétentes" à l'article 26, 7^e de la LPD, à savoir *"les services de police au sens de l'article 2, 2^e, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux"*. Les deux ministres de tutelle ont bien la responsabilité (politique) finale, mais les services de police doivent quand même au moins être

désignés comme responsables du traitement opérationnels en vertu de l'article 26, 7° de la LPD *juncto* l'article 2, 2° de la LPI, si pas être considérés comme responsables du traitement conjoints). Ils ont en effet une influence de fait sur le traitement et contribuent au moins à déterminer dans les faits les moyens mis en œuvre en vue des finalités visées. On peut également s'inspirer des termes "gestionnaire" et "responsable opérationnel" employés pour les banques de données communes, outre le responsable du traitement proprement dit. Une telle construction est préférée par le COC pour la BNG et les banques de données de base et même pour les banques de données particulières. Pour assurer une uniformité entre les différentes banques de données policières, le COC choisit de désigner comme responsable du traitement la zone de police (pour la police locale) et le Ministre de l'Intérieur et/ou de la Justice (pour la police fédérale). Le chef de corps, le commissaire général, le directeur général et les directeurs sont alors les responsables opérationnels et les gestionnaires. Ainsi, il y a une uniformité juridique dans la désignation du responsable du traitement, du responsable opérationnel et du gestionnaire pour l'ensemble des banques de données policières et communes.

Le 2° paragraphe prévoit que pour toutes les banques de données mentionnées à l'article 44/2 (à savoir la BNG, les banques de données de base, les banques de données particulières, les banques de données communes et les banques de données techniques), les deux ministres déterminent par directives – le COC aurait aimé lire "par directives contraignantes" – les mesures en vue d'assurer la gestion et la sécurité, et que pour tout traitement dans les banques de données précitées, des fichiers de journalisation soient établis pour les traitements les plus essentiels. Il n'est tout d'abord pas recommandé de paraphraser/copier l'actuel article 56 de la LPD dans le 3° alinéa du § 2 ; un simple renvoi à cet article 56 LPD suffit.

Ces fichiers de journalisation doivent ensuite permettre de générer les informations prévues par le projet de 3° alinéa (superflu) du § 2, ce que le COC salue dès lors qu'à l'heure actuelle, ce n'est pas possible de le faire avec autant de détails. Il s'agit donc d'une finalité ambitieuse qui devra également être concrétisée et pour laquelle les responsables du traitement pourront être interpellés. Ainsi par exemple, la mention d'un motif d'un traitement (par exemple dans la BNG) n'est jusqu'à présent pas encore une obligation à laquelle on ne peut échapper. À l'heure actuelle il s'agit d'une possibilité facultative qui n'est pas toujours respectée, mais rien n'empêche un agent de police d'indiquer un faux motif. En ce qui concerne les fichiers de journalisation, le COC souligne qu'il doit y avoir accès à tout moment, comme l'affirme aussi l'Exposé des motifs, même si un code utilisateur limité est prévu pour l'information.

Le projet de § 3 est également nouveau. Il impose aux ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences, de déterminer par directive les règles d'accès des membres des services de police aux banques de données visées à l'article 44/2, § 1 et § 3. La circulaire MFO 3, qui est désespérément désuète depuis bien longtemps et qui n'a pas été adaptée suite aux modifications du cadre juridique en matière de gestion de l'information apportées par la loi de 2014¹⁰, nécessite par cet avant-projet une mise à jour encore plus profonde, qui devra intégrer aussi cet aspect des règles d'accès. Les responsables du traitement pourront également être interpellés à ce sujet.

L'Exposé des motifs motive de manière étendue la raison pour laquelle des liens entre différentes banques de données policières et autres ou entre parties de celles-ci sont nécessaires dans son commentaire du projet de § 3bis de l'article 44/4 qui est une paraphrase de l'actuel § 3. Le COC comprend parfaitement le raisonnement mené mais insiste pour que les ministres de tutelle exercent aussi réellement cette compétence en formulant des directives et en n'acceptant pas que des liens

¹⁰ 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 de données à caractère personnel et le Code d'instruction criminelle.

soient établis sur le terrain qui ne soient pas encadrés par de telles directives, ce qui est le cas actuellement. L'exemple le plus évident est l'application INFOTHÈQUE au sein de laquelle les banques de données de base de dizaines de zones de police sont reliées en l'absence de telles directives. En l'espèce, c'est d'autant plus problématique que les banques de données de base précitées contiennent encore beaucoup d'informations non validées. La nécessité opérationnelle de disposer aussi dans certains cas d'informations non validées est évidente, mais la nécessité de règles contraignantes concernant l'accès et l'utilisation de ces données non validées sont d'autant plus indispensables. À cet égard, le COC renvoie à l'enquête de contrôle 2016/1 qu'il a menée.

Les exemples donnés dans l'Exposé des motifs vont encore bien plus loin et s'inscrivent dans le cadre du concept "I-police" où un fonctionnaire de police a accès sur le terrain via sa tablette ou son smartphone à une foule d'informations et de fichiers de données. On y trouvera aussi inévitablement des informations qui ne sont pas encore évaluées et/ou validées, ce qui, comme l'affirme l'Exposé des motifs à juste titre, est *"particulièrement important dans des situations de contrôle pouvant avoir des effets sur les droits et libertés des personnes"*. Ceci devra être bien encadré par les directives annoncées. Entre-temps, en ce qui concerne INFOTHÈQUE par exemple, quelques conventions policières internes ont quand même été conclues, mais cela est largement insuffisant. L'application FOCUS, qui est notamment utilisée par la police d'Anvers et par laquelle l'inspecteur de police peut consulter directement sur sa tablette/son smartphone toutes sortes d'informations provenant de différentes banques de données, est également juridiquement problématique à l'heure actuelle, bien qu'en termes opérationnels, on ne puisse douter de sa plus-value. Il ne suffit donc pas de donner une délégation aux ministres de tutelle dans une législation ; elle doit aussi être **exécutée** en pratique, ce qui est d'autant plus le cas au regard du projet de 2^e alinéa du § 3bis. Depuis 2014, force est de constater que les choses laissent à désirer à ce niveau.

Le COC souhaite dès lors exhorter les ministres de tutelle à concrétiser enfin les directives précitées qui devront, encore bien plus qu'auparavant, comporter toute une série d'éléments détaillés comme décrit précisément dans les projets de §§ 3, 3bis et 3ter de l'article 44/4 et dans l'Exposé des motifs y afférent.

En ce qui concerne enfin le projet d'article 44/4 § 3, 3bis et 3ter de la LFP, l'Organe de contrôle formule des réserves explicites quant à la question de savoir si l'avant-projet offre bien une base légale (suffisante) pour instaurer le futur concept "I-police", ce que l'Exposé des motifs s'empresse de supposer à tort (p. 14). À l'heure d'aujourd'hui, il n'est pas encore suffisamment évident de savoir ce que comportera précisément le concept précité (en réalité), empêchant *hic et nunc* le COC d'évaluer suffisamment sa compatibilité avec la LFP, la LPD et le RGPD.

9. À l'article 44/5, une 7^e catégorie de données à caractère personnel qui peuvent être traitées à des fins de police administrative est ajoutée, à savoir *"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 en vertu de la loi"*. Les finalités de la reprise de cette nouvelle catégorie dans la BNG et les banques de données de base sont commentées en détail dans l'Exposé des motifs.

La notion de *"mesure administrative"* n'est pas définie dans la LFP (voir les définitions à l'article 3¹¹). Cette notion est toutefois utilisée à l'article 30 de la LFP (en ce qui concerne la saisie administrative, où la notion est néanmoins clairement utilisée dans sa signification la plus restreinte de mesure

¹¹ La notion de "mesure policière" est bien définie mais est clairement plus restreinte que celle de mesure administrative. Une mesure policière doit émaner d'une autorité de police administrative ou judiciaire, ce qui n'est pas nécessairement le cas pour une mesure administrative qui peut émaner par exemple d'une administration ordinaire.

policière (administrative) prise par un fonctionnaire de police). L'utilisation à l'article 44/9 (concernant l'archivage des données de la BNG) semble plus importante. Il y est question d'une *"mesure sur la base d'une décision d'une autorité administrative ou judiciaire compétente"* (cf. l'art. 44/9, § 1, 2^e alinéa, a) et § 2, 4^e alinéa, 1^e tiret et 7^e alinéa, 1^e tiret), mais il faut partir du principe que le législateur parle ici d'une mesure prise par une autorité policière (administrative) au sens de l'article 3, 2^o de la LFP.

L'Exposé des motifs établit toutefois clairement que l'on vise en l'espèce une catégorie encore plus large de décisions mais il reste quelque peu vague étant donné qu'il donne quelques exemples non exhaustifs. Quelques uns de ces exemples ne sont en outre pas une mesure administrative mais purement une sanction administrative, dont l'Exposé des motifs donne d'ailleurs aussi un exemple concret (à savoir les sanctions prévues dans la loi SAC du 24 juin 2013). Il est crucial de savoir **clairement** dans la loi quelles mesures et sanctions de quelles autorités peuvent être saisies dans la BNG et dans les banques de données de base. En ce sens, le COC propose de faire la clarté et de compléter le point 7^o par le terme *"sanction"* et de reformuler légèrement comme suit : *"les données relatives aux personnes faisant l'objet d'une mesure administrative ou d'une sanction administrative prise par une autorité administrative compétente et que les services de police doivent surveiller par ou en vertu de la loi ou dont ils assurent le respect."* De cette manière, on sait clairement qu'il ne s'agit pas uniquement de décisions prises par une autorité policière administrative (bourgmestre, gouverneur, ministre de l'Intérieur) mais par toute administration qui peut prendre une mesure ou une sanction dont la surveillance du respect ou de l'application relève des missions de la police, et ce par ou en vertu de la loi.

Les autres modifications de l'article 44/5 ne donnent pas lieu à des remarques spécifiques.

10. À l'article 44/9 concernant l'archivage et l'effacement des données dans la BNG, quelques modifications sont apportées (que l'on appelle souvent dans le jargon policier *"ventilation"*). On prévoit que la nouvelle catégorie de mesures administratives (et de sanctions, cf. plus haut) soit ventilée après 3 ans au plus tard. Contrairement à ce que mentionne l'Exposé des motifs, il ne s'agit pas d'une *"adaptation technique"*. Le COC prend acte du choix du délai le plus court de 3 ans qui est en effet un délai maximal. Il incombe à l'auteur du projet d'évaluer si la ventilation après 3 ans correspond dans tous les cas à la durée de la mesure. Le COC ne connaît pas toutes les mesures potentielles existantes que la police doit surveiller mais constate néanmoins que les plus récurrentes sont d'une durée inférieure à 3 ans (fermeture d'institution, suspension d'autorisation d'exploitation, interdiction de lieu, ...). Mais ce n'est pas toujours le cas. On constate ainsi que la source authentique des interdictions de stade administratives (loi football) qui se trouve au SPF Intérieur prévoit un délai de conservation de 5 ans¹² étant donné qu'une interdiction de stade (administrative) à titre de sanction peut être infligée pour une durée allant jusqu'à cinq ans maximum.

Dans la pratique, le COC constate quoi qu'il en soit que, sauf pour des adaptations ponctuelles à l'occasion par exemple d'une demande d'accès indirect, les délais de ventilation maximaux utilisés à l'article 44/9 sont bel et bien épuisés. Vu la masse de données, l'obligation du responsable du traitement (en l'espèce les services de la police intégrée) d'archiver dès que les données présentent un caractère non adéquat, non pertinent ou excessif est en pratique manifestement tout à fait irréalisable.

En pratique, il apparaît en outre que les règles de ventilation qui sont déjà d'application depuis 2014 ne sont appliquées que depuis très récemment et de surcroît de manière très partielle seulement, ce

¹² Article 1, § 4 de l'arrêté royal du 7 décembre 1999 *contenant l'établissement d'un fichier des interdictions de stade*.

qui constitue quand même un problème majeur que l'Organe de contrôle a déjà mis en évidence de manière répétée. Ce n'est que le 20 novembre 2018 que les données à caractère personnel de police administrative ont été ventilées de manière systématique, comme le prévoit l'article 44/9 de la LFP. Il s'agissait, pour autant que l'Organe de contrôle ait pu le constater, d'une opération "one shot". Les données à caractère personnel de police judiciaire ne sont toujours pas ventilées, et encore moins de manière systématique. Son application automatisée ne serait prête qu'à la mi 2019, à titre ou non de mesure "one shot". Il est évident que tout cela est de plus en plus problématique, d'autant plus depuis l'entrée en vigueur du nouveau cadre de protection des données. L'Organe de contrôle acceptera encore une période de tolérance jusqu'à la mi 2019 mais recourra ensuite au besoin à ses possibilités de sanction administrative et à ses compétences correctrices. Il doit en effet être clair que la non-application des règles de ventilation est tout à fait contraire notamment avec les articles 28, 1°, 2°, 3° et 4°, 29, § 5 et 30, 1° alinéa de la LPD (et les articles 4 et 5 correspondants de la Directive Police et Justice). Ce n'est pas le lieu pour aborder cette problématique en profondeur, ce que l'Organe de contrôle fera dans le cadre d'une enquête thématique spécifique sur l'application des règles de ventilation par les services de la police intégrée.

Toutefois, une des principales raisons pour lesquelles la police et ses autorités de tutelle sont restées en défaut, depuis 2014 à aujourd'hui, de respecter un principe fondamental du droit de protection des données touche principalement à la complexité des règles de ventilation dans la LFP. Le COC a déjà adressé un courrier à la police fédérale à ce sujet il y a une paire d'années pour demander d'envisager une simplification du système, courrier qui a toutefois reçu une réponse négative. Il est cependant clair que plus un règlement est complexe, plus son respect sera problématique et plus il sera néfaste pour la vie privée. Vu le caractère nécessairement automatisé de la ventilation des millions de données, il est important d'avoir un système de délai qui ne soit pas trop complexe. Le résultat de la situation actuelle prédit par l'Organe de contrôle, à savoir que les règles légales ne seront simplement pas appliquées, s'est aussi confirmé depuis 2014 à aujourd'hui. En l'espèce, le COC renouvelle son appel à simplifier les règles de ventilation légalement prévues. Cette simplification est en parfaite adéquation avec (l'ancien et le nouveau) cadre de protection des données et porte le moins atteinte à la vie privée, bien au contraire. Récemment, la Cour constitutionnelle a estimé ce qui suit dans son arrêt 29/2018, en ce qui concerne le délai de conservation de données de consommation d'eau, d'électricité et de gaz qui sont transmises aux autorités depuis les entreprises d'utilité publique ou les gestionnaires de réseaux de distribution dans le cadre de la lutte contre la fraude au domicile : *"Compte tenu du fait que le législateur ne peut prévoir des règles distinctes et précises pour tous les cas spécifiques, il pouvait régler de manière générale les conditions de conservation des données à caractère personnel, ainsi que la durée de cette conservation. Il découle de ce qui précède que le législateur a réglé les éléments essentiels de la durée de conservation des données."* (considérant B.23).

Par ailleurs, l'Organe de contrôle se demande si l'ensemble du système d'archivage tel que prévu dans la LFP est encore compatible avec l'article 30 de la LPD qui affirme dans son 1° alinéa qu'à l'échéance de cette durée de conservation, les données sont effacées. Un archivage général et non ciblé de toutes les données semble contraire à cette disposition. Certes, le 2° alinéa de l'article 30 de la LPD prévoit la possibilité que la loi puisse prévoir qu'à l'échéance d'un premier délai de conservation, une analyse doit être 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, mais le constat reste que dans la LFP, on ne trouve rien quant à de tels "critères différents de nécessité et de proportionnalité", et ils ne sont pas non plus appliqués en pratique, pour autant déjà qu'ils existent. En principe, toutes les données à caractère personnel et informations sont en effet archivées sans un quelconque contrôle de nécessité et de proportionnalité. La LPD est en l'espèce la transposition notamment des articles 4 et 5 de la Directive Police et Justice qui concernent à leur tour une **vérification régulière** de la conservation des données, un système d'archivage automatique de

toutes les données après une échéance déterminée étant également contraire à ce principe. Il incombe à l'auteur du projet de faire la clarté à cet égard.

11. Dans le projet d'article 44/11/2 (article 13 de l'avant-projet) au 2^e paragraphe, l'actuel 1^e alinéa est supprimé, lequel dispose que "*Les données à caractère personnel et les informations traitées dans les banques de données de base, à l'exception de celles relatives à la gestion des enquêtes, ne sont disponibles et directement consultables que par les services de police qui les ont enregistrées ou qui doivent, de par leurs missions légales, coordonner les données et informations.*" De cette manière, l'auteur du projet veut retirer de la zone d'ombre légale la pratique actuelle - problématique du point de vue légistique - de couplage entre les banques de données de base ISLP des différentes zones de police locales (cf. ci-avant, l'enquête INFOTHÈQUE du COC). Le COC a lui-même plaidé pour cela dans son enquête de contrôle dès lors que la plus-value opérationnelle de tels couplages est incontestable, mais engendre par ailleurs aussi des risques plus élevés au niveau de la vie privée et de la protection des données, l'application précitée étant un exemple type de cas dans lesquels la police travaillera avec des informations non validées et posera probablement aussi certains actes policiers avec exercice ou non de la contrainte ou de la violence. D'où la nécessité d'intégrer dans ces cas les limites et sécurités utiles dont question ci-avant (cf. point 8).

12. À l'article 44/11/3 de la LFP qui régit les banques de données particulières (article 14 de l'avant-projet), le premier paragraphe est remplacé et l'on indique surtout quelles catégories de données peuvent y être reprises. L'Organe de contrôle, depuis qu'il a rendu son avis le 31 mars 2017 sur environ 800 banques de données particulières, plaide pour la suppression des termes "*dans des circonstances exceptionnelles*" comme condition pour la création d'une banque de données particulière.

Tout d'abord, personne ne sait vraiment, et certainement pas la police, ce que l'on doit entendre par "*circonstances exceptionnelles*". Lors de la déclaration de dizaines de banques de données particulières, l'Organe de contrôle a déjà aussi été en conflit avec cette notion, d'autant plus que de nombreuses déclarations ne reflétaient rien d' "exceptionnel", mais faisaient simplement partie du fonctionnement régulier de la police. En d'autres termes, de très nombreuses banques de données particulières font partie de ce qu'on peut considérer comme des missions de routine et des compétences d'un service de police dans l'exercice normal des tâches de police administrative et judiciaire. Étant donné toutefois que le fichier de données déclaré ne peut être considéré comme faisant partie ni d'une banque de données de base, ni de la BNG, bon nombre d'entre eux ont quand même été considérés comme une banque de données particulière par l'Organe de contrôle parce qu'autrement, on aurait pu penser que le fichier n'aurait tout simplement aucune base juridique étant donné que l'énumération des banques de données policières existantes est une énumération limitative. On peut citer comme exemple les banques de données particulières reprenant des données de trans migrants ou de personnes pour lesquelles il y a des indices de radicalisation, ou une banque de données à caractère personnel liées à des bateaux et à leurs propriétaires, ou la banque de données "Mercure" pour la gestion des données d'une enquête sur la téléphonie, ou une banque de données de personnes qui habitent la zone et à l'égard desquelles des mesures de probation ont été prononcées, une banque de données pour le management RIR¹³ (management d'informations douces), une banque de données des permis de conduire retirés immédiatement, une banque de données de personnes sous surveillance électronique, la banque de données "infocop" qui est plutôt un outil de briefing avec toutes sortes d'informations opérationnelles, une banque de données "attention particulière" dont le but est de diriger des équipes d'intervention et d'action et qui reprend un relevé

¹³ Pour "Rapport d'Information-Informatierapporten".

des personnes, lieux et véhicules qui doivent faire l'objet de l'attention particulière des équipes, une banque de données des mineurs placés sous surveillance, etc. On pourrait donner ainsi des dizaines d'exemples. Toutes ces banques de données sont nécessaires pour l'exercice courant et régulier des missions de police et ne constituent dès lors pas véritablement des "*circonstances exceptionnelles*".

Pour ne pas dévaluer le concept de banque de données "*particulière*", l'Organe de contrôle a toutefois estimé à de très nombreuses reprises qu'il ne s'agissait pas de banques de données particulières mais que la police devait quand même pouvoir les maintenir, parce qu'elles sont nécessaires pour son fonctionnement (bien que, comme indiqué, on peut douter quant à l'existence d'une base juridique pour la police pour maintenir une banque de données opérationnelle, autre que les types énoncés dans la LFP). Il s'agissait par exemple d'une banque de données de personnes arrêtées administrativement (registre des personnes arrêtées), d'une banque de données de visiteurs d'un poste de police, d'un registre d'objets saisis, d'une banque de données d'infractions commises par des véhicules prioritaires, etc.

Il serait plus confortable pour tout le monde sur le terrain si la notion de "*circonstances exceptionnelles*" était abandonnée, ou du moins si elle était remplacée par une description plus proche de la réalité et mieux utilisable tant pour la police que pour le COC, comme par exemple la notion de "dans des circonstances spécifiques, ...". L'Exposé des motifs parle d'ailleurs à juste titre de la "*spécificité des banques de données particulières*", ce qui est plus correct que leur prétendu caractère exceptionnel. Pour le reste, les besoins particuliers prévus au § 2 restent d'application.

Dans le paragraphe 3 modifié, la déclaration préalable de la banque de données particulière au COC est abrogée, avec la justification sommaire que "*ceci ne correspond plus au système établi par la loi relative à la protection des données*". Cependant, ni la Directive Police et Justice, ni le titre 2 de la LPD n'interdisent d'instaurer un système d'avis préalable pour certaines banques de données. Le système de consultation préalable de l'autorité de contrôle tel que prévu à l'article 58 et à l'article 59 de la LPD (à savoir lorsqu'un traitement présente probablement un risque élevé pour les droits et libertés de personnes physiques, en combinaison avec les conditions telles que prévues à l'article 59 de la LPD) ne peut être comparé au système existant de déclaration préalable de la LFP et à l'avis consécutif du COC. Quoi qu'il en soit, le COC a l'intention de suivre cela de près via l'application de l'article 59, § 2¹⁴. Pour l'Organe de contrôle, toutes les banques de données particulières sont en principe des traitements pour lesquels une consultation préalable est nécessaire.

Néanmoins, dans le cadre de la simplification administrative en faveur des services de police et de l'Organe de contrôle (qui lui-même ne peut plus tenir de registre), le COC peut se retrouver dans un accès via le registre des traitements des services de police comme établi dans le nouveau projet d'article 145 de la LPI. Il doit alors être clair que ledit registre doit contenir toutes les données que la déclaration actuelle au COC contient, ce qui n'est pas le cas à première vue. L'Organe de contrôle a vu une première démonstration du registre par la police fédérale et il est apparu d'emblée que les informations qui s'y trouvent sont trop sommaires que pour permettre à l'Organe de contrôle de réaliser une (première) évaluation en connaissance de cause (autrement dit, sans devoir vérifier sur place dans la banque de données).

13. À l'article 44/11/3ter, § 1 de la LFP, qui comporte une description des services/organismes qui ont un accès direct aux banques de données communes, cet accès fait défaut à l'heure actuelle, tant pour le COC que pour le Comité permanent R. Chez le gestionnaire de la banque de données, à savoir la

¹⁴ "L'autorité de contrôle compétente peut établir une liste des opérations de traitement devant faire l'objet d'une consultation préalable conformément au paragraphe 1."

police fédérale, on débat sur la question de savoir s'il y a actuellement une base juridique pour les deux instances de contrôle pour disposer d'un accès direct. Il incombe en effet à la police fédérale de veiller au niveau technique à ce que cet accès soit donné.

Pour le COC, cette base juridique est limpide étant donné qu'au § 1, 1^e alinéa, il est littéralement question d'un accès pour "l'organe", qui ne peut viser ici que le COC. Étonnamment toutefois, le Comité R n'y est pas repris, une erreur manifestement. Quoi qu'il en soit, l'occasion est idéale pour faire la clarté et pour prévoir expressément l'accès direct, tant pour le COC que pour le Comité permanent R. Cela peut se faire soit dans cet article, soit dans le projet d'article 44/11/3quinquies/2 de la LFP. Le fait que les deux organes de contrôle aient besoin d'un tel accès direct ne peut être mis en doute. Un contrôle sérieux n'est possible que si l'autorité de contrôle dispose du même accès que les services de base. Tant le RGPD que la Directive Police et Justice prévoient d'ailleurs que l'autorité de contrôle doit disposer de "*pouvoirs d'enquête effectifs*". Le COC a d'ailleurs déjà un accès direct à la BNG. Le COC préfère clairement une disposition spécifique expresse dans le projet d'article 44/11/3quinquies/2 de la LFP, où l'on pourrait insérer l'alinéa suivant entre le 1^e et le 2^e alinéa (qui deviendrait le 3^e alinéa) : "*Sur la base du besoin d'en connaître, tout ou partie des données à caractère personnel et des informations des banques de données communes sont directement accessibles à tout moment à l'Organe de contrôle et au Comité permanent de contrôle des services de renseignements. Le gestionnaire assure la mise en place de l'accès direct précité.*"

À cet égard, le début dudit article et notamment les termes "*Dans le respect de l'exercice de leurs missions respectives*", manquent de clarté. Les deux autorités de contrôle peuvent exercer leurs compétences respectives (reprises dans la LPD pour le COC et dans la loi du 18 juillet 1991 pour le Comité R) lors du contrôle des banques de données communes. Il conviendrait de le formuler comme suit : "*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, conformément à leurs compétences prévues respectivement dans la loi relative à la protection des données et dans la loi du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace, par l'Organe de contrôle et le Comité permanent de contrôle des services de renseignements tel que visé à l'article 28 de la loi précitée du 18 juillet 1991.*"

Par souci d'exhaustivité, l'Organe de contrôle souhaite faire remarquer que les références à "l'Organe" à l'article 44/11/3ter, § 4 et à l'article 44/11/3quater reposent manifestement sur une erreur. La référence à l'Organe de contrôle doit être supprimée dans cette disposition. L'Organe de contrôle constate enfin que l'actuel article 44/11/3quinquies de la LFP n'est pas modifié par le projet bien que son 2^e alinéa renvoie encore à la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* qui a entre-temps été abrogée. L'auteur du projet se devra d'adapter cette disposition au nouveau cadre législatif en vigueur.

14. Dans la version néerlandaise du projet d'article 44/11/8bis (article 21 de l'avant-projet), aussi bien à l'alinéa 1 qu'à l'alinéa 2, les termes "*veiligheidsdiensten*" doivent être remplacés par les termes "*inlichtingen- en veiligheidsdiensten*". Cette disposition doit quoi qu'il en soit être lue conjointement avec le projet modifié d'article 44/11/12 (article 23 de l'avant-projet).

De manière plus fondamentale, le COC constate avant tout un manque de réciprocité équivalente dans les accès que l'on veut octroyer réciproquement aux banques de données respectivement des services de police et des services de renseignement. Alors que les services de renseignement obtiendraient la forme la plus aboutie de communication d'informations policières via un accès direct, le mouvement inverse, à savoir un accès (direct) pour les services de police aux banques de données des services de renseignement resterait dans le flou et serait relégué à un "*protocole d'accord*" qui doit entrer en

vigueur simultanément avec celui de l'accès direct à la BNG au profit des services de renseignement. Le renvoi aux articles 19 et 20 de la loi organique des services de renseignement et de sécurité¹⁵ du 30 novembre 1998 est également très peu explicite. Ainsi, le projet semble vouloir accorder davantage de protection/cloisonnement à l'information des services de renseignement qu'aux informations policières. Indépendamment du fait que l'on ne trouve aucune justification de ce choix dans l'Exposé des motifs, le COC s'interroge sérieusement à cet égard. L'échange d'informations plus performant propagé dans l'Exposé des motifs, qui a en effet été recommandé par la Commission d'enquête parlementaire attentats, n'est manifestement valable que dans un seul sens principalement (de la police vers les services de renseignement). Par ailleurs, le 1^e alinéa fait double emploi avec l'article 14 de la LRS.

Laisser fixer les modalités de communication des données (à noter que le terme "*données*" est aussi bien plus vague que le mouvement inverse où "*des données à caractère personnel et des informations*" seraient directement accessibles pour les services de renseignement) dans un protocole d'accord est quoi qu'il en soit contraire au principe de légalité et à l'article 22 de la Constitution¹⁶. Étant donné que le COC n'a aucune idée de ces modalités (s'agit-il aussi d'un accès direct, uniquement d'une consultation ou d'une communication ponctuelle quelque peu structurée ?), il n'est pas en mesure d'évaluer correctement ledit flux de données vers la police. L'Exposé des motifs n'apporte pas plus de clarté sur ce point.

¹⁵ Ci-après "LRS".

¹⁶ De nombreux arrêts de la Cour constitutionnelle indiquent comment il convient de comprendre cela. À cet égard, on peut de nouveau se référer à l'arrêt 29/2018 (Considérents B 13.1 et B 13.2) et à toutes les références à la jurisprudence de la Cour européenne des droits de l'homme et de la Cour de justice qui y sont énumérées) : "*En réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée, l'article 22 de la Constitution garantit à tout citoyen qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue.*

Une délégation à un autre pouvoir n'est toutefois pas contraire au principe de légalité pour autant que l'autorisation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur.

Outre l'exigence de légalité formelle, l'article 22 de la Constitution impose également que l'ingérence dans l'exercice du droit au respect de la vie privée soit définie en des termes clairs et suffisamment précis qui permettent d'appréhender de manière prévisible les hypothèses dans lesquelles le législateur autorise une pareille ingérence.

De même, l'exigence de prévisibilité à laquelle la loi doit satisfaire pour être jugée conforme à l'article 8 de la Convention européenne des droits de l'homme implique que sa formulation soit assez précise pour que chacun puisse - en s'entourant au besoin de conseils éclairés - prévoir, à un degré raisonnable, dans les circonstances de la cause, les conséquences d'un acte déterminé (CEDH, grande chambre, 4 mai 2000, Rotaru c. Roumanie, § 55 ; grande chambre, 17 février 2004, Maestri c. Italie, § 30). La législation doit donner à chacun une indication suffisante sur les circonstances dans lesquelles et à quelles conditions elle habilite la puissance publique à recourir à des mesures affectant les droits protégés par la Convention (CEDH, grande chambre, 12 juin 2014, Fernández Martínez c. Espagne, § 117).

Plus particulièrement, lorsque l'intervention de l'autorité présente un caractère secret, la loi doit offrir des garanties suffisantes contre les ingérences arbitraires dans l'exercice du droit au respect de la vie privée, en délimitant le pouvoir d'appréciation des autorités concernées avec une netteté suffisante, d'une part, et en prévoyant des procédures qui permettent un contrôle juridictionnel effectif, d'autre part (CEDH, grande chambre, 4 mai 2000, Rotaru c. Roumanie, § 55 ; 6 juin 2006, Segerstedt-Wiberg c. Suède, § 76 ; 4 juillet 2006, Lupsa c. Roumanie, § 34).

En ce moment, les services de renseignement disposent déjà d'une base juridique pour une interrogation directe de la BNG, et ce depuis avril 2014. Mais pour des raisons que le COC ignore, ce n'est pas appliqué en pratique. C'est ce que reconnaît l'Exposé des motifs, bien que de manière implicite, qui précise que l'échange d'informations est à présent réalisé *"par des mécanismes ad hoc au travers de relais formels ... 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 ..., mais souvent aussi à la demande d'un enquêteur des services de renseignements ..."* (p. 31). On ne sait donc pas clairement si le système existant d'interrogation directe de la BNG via une fonction *"hit no hit"* pour les services de renseignement est insuffisant et dans l'affirmative, pourquoi ce le serait. Par souci de clarté, une interrogation directe de la BNG permet déjà énormément de choses. Elle permet aux services de renseignement, en vertu de l'article 44/11/4, § 3 de la LFP, de disposer d'un accès direct *"à tout ou partie des données suivantes :*

- a) l'existence de données sur une personne en application de l'article 44/5, § 1er, alinéa 1er, 2° à 6°, et § 3, 1° à 9° ;*
- b) la qualification retenue par la police concernant les faits pour lesquels la personne est enregistrée ;*
- c) les données nécessaires pour obtenir plus d'informations auprès de l'autorité compétente ; et*
- d) les données relatives aux mesures à prendre pour les personnes visées au point a)",* sur la base de quoi les services de renseignement peuvent prendre contact avec le service de police – ou le fonctionnaire – concerné pour obtenir des informations encore plus détaillées.

Avant même qu'il soit établi clairement ou du moins de manière acceptable que l'interrogation directe ne permettrait pas aux services de renseignement de réaliser leurs missions correctement, ni pour quelle raison ces possibilités ne sont manifestement pas exploitées en pratique, la BNG est **entièrement** "ouverte" aux services de renseignement par une consultation directe. Contrairement à ce que l'Exposé des motifs semble affirmer, cette extension est bel et bien très importante et place les services de renseignement en tant qu'organes exécutifs au même rang que les autorités administratives et judiciaires et les organes de contrôle indépendants. Pour l'OCAM, il semble y avoir moins d'objections parce que l'OCAM n'est pas un service de renseignement avec des compétences opérationnelles. Une consultation directe permet quoi qu'il en soit aux services de renseignement de prendre connaissance de tous les antécédents policiers et judiciaires d'une personne concernée, même de ceux qui n'ont absolument rien à voir (par exemple des faits de mœurs purs, des faux de droit commun, des infractions routières, la fraude fiscale et sociale ordinaire, etc.) avec les compétences des services de renseignement, et ce sans appliquer le moindre filtre, ce qui n'est pas le cas lors de l'interrogation directe en vigueur actuellement. Le fait que l'accès soit "limité" à certains agents des services de renseignement qui sont titulaires d'une habilitation du degré très secret n'enlève rien à ce constat. La toute grande majorité des membres des services de renseignement disposent d'une telle habilitation et les possibilités d'accès direct à la BNG vaudront pour la toute grande majorité de ces membres du personnel (aussi bien les services extérieurs que les services d'analyse).

Pour l'Organe de contrôle, tout cela est contraire au principe de proportionnalité et de finalité, à l'article 22 de la Constitution (lu en combinaison ou non avec l'article 8 de la CEDH, l'article 17 du Pacte DCP et les articles 7 et 8 de la Charte européenne des droits fondamentaux) et est encore moins de nature à *"préserver la présomption d'innocence et le droit au respect de la vie privée"*, dont question dans l'Exposé des motifs.

Par souci d'exhaustivité, le COC souligne que l'accès direct envisagé pour les services de renseignement est bien limité à la BNG. En ce sens, le passage de l'Exposé des motifs indiquant *"dont celles figurant*

dans la BNG" prête à confusion. Pour une bonne compréhension, il incombe d'ailleurs à l'auteur du projet de clarifier les choses. S'agit-il de l'accès direct envisagé ou encore d'autres banques de données en dehors de la BNG et des banques de données techniques ?

15. Les modifications envisagées de l'article 44/11/9, § 1 de la LFP s'inscrivent dans le prolongement des modifications prévues à l'article 44/11/8 et au nouvel article 44/11/8bis de la LFP.

Au 2^e paragraphe, le présent avant-projet est toutefois l'occasion de transposer l'arrêt 108/2016 du 14 juillet 2016 de la Cour constitutionnelle dans le texte légal en faisant suivre le terme "avis" du terme "**contraignant**" afin que le texte de ce paragraphe devienne : "**§ 2. Après avis contraignant de l'Organe de contrôle, 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.**" De la sorte, on donne suite à l'arrêt précité qui indiquait notamment ce qui suit au sujet de cette disposition en ce qui concerne la communication de données à caractère personnel des banques de données policières aux autorités publiques/organes/institutions belges :

"Bien que l'article 44/11/9, § 2 de la loi sur la fonction de police prévoie qu'une telle communication n'est possible qu'après avis de l'Organe de contrôle de l'information policière, il ne ressort pas de cet article si l'avis est contraignant ou non. Dans la mesure où l'avis ne serait pas contraignant, la disposition attaquée pourrait donner lieu à des communications de données à caractère personnel provenant des banques de données policières qui, de l'avis de cet Organe de contrôle, ne sont pas conformes aux dispositions de la loi attaquée, par exemple parce que l'autorité qui demande la communication des données à caractère personnel n'a pas besoin de ces données pour l'exécution de sa mission légale et ne justifie ainsi pas du "besoin d'en connaître" (voy. les travaux préparatoires reproduits en B.98.4.4). Dans l'interprétation précitée, l'article 44/11/9, § 2 de la loi sur la fonction de police causerait une ingérence disproportionnée dans l'exercice du droit au respect de la vie privée."

"Ce n'est que dans la mesure où l'avis de l'Organe de contrôle est considéré comme contraignant pour les autorités qui sont compétentes pour communiquer des données à caractère personnel provenant des banques de données policières aux autorités, organes et organismes visés dans l'article 44/11/9, § 2, que cet article n'a pas d'effet disproportionné au regard des objectifs du législateur. Sous réserve de cette interprétation, cet article est compatible avec les dispositions constitutionnelles et conventionnelles mentionnées en B.7" (considérants B. 99.3.3 en B.99.3.4). Le terme "avis" a donc le sens d' "autorisation" ou d' "avis contraignant". Le COC exhorte l'auteur du projet à donner suite à l'arrêt précité de la Cour constitutionnelle.

16. La modification technique de l'article 44/10/10 (article 22 de l'avant-projet) de la LFP est l'occasion pour le COC d'attirer l'attention sur la problématique actuellement très préoccupante de la communication de données à caractère personnel policières à des institutions pour la recherche scientifique ou à des chercheurs d'instituts scientifiques, une communication entourée d'une très grande insécurité juridique. À ce sujet, l'avis COC-CONTROLE-002-2018 du 23 octobre 2018 a été remis à l'auteur du projet. Ladite disposition prévoit qu'un arrêté royal, après avis (à l'avenir) de l'Organe de contrôle, précisera les institutions ou personnes auxquelles peuvent être communiquées les données à caractère personnel qui sont nécessaires pour accomplir les missions d'intérêt public liées à la recherche scientifique qui leur sont confiées par ou en vertu d'une loi, d'un décret ou d'une ordonnance. Cet arrêté devra également préciser les modalités de cette communication.

Cette disposition, qui est entrée en vigueur le 7 avril 2014, n'a jamais été exécutée jusqu'à présent, de sorte qu'au sens strict, on ne peut pas transmettre des données policières aux chercheurs d'universités ou de hautes écoles, ce qui pose bien entendu des problèmes majeurs pour la recherche scientifique

de même que pour les services de police. Actuellement, on peut se tirer d'affaire par le biais d'autorisations ponctuelles du ministère public compétent, pour autant que les données policières se trouvent sur le procès-verbal et fassent donc partie d'un dossier pénal. Si tel n'est toutefois pas le cas, par exemple s'il s'agit de données sur les patrouilles, les lieux d'interventions et les types d'interventions, etc., un véritable problème juridique se pose. Le COC a déjà été interrogé à ce sujet par exemple par l'Université de Gand, qui veut réaliser au sein de la zone de police d'Anvers – et à la demande de cette dernière – une recherche scientifique sur les possibilités et limitations du concept appelé "predictive policing", nécessitant une multitude de données policières, dont des données à caractère personnel. À défaut d'arrêté d'exécution, de telles recherches sont soumises à de grandes incertitudes ou la police refuse de fournir ces données du fait que l'existence d'un fondement juridique suffisant n'est pas garantie.

Cette absence d'arrêté d'exécution est d'autant plus singulière que, pour d'autres services de sécurité, comme par exemple les services de renseignement ou l'OCAM, la LPD a bel et bien prévu un règlement spécifique pour l'utilisation des données traitées par ces institutions à des fins scientifiques. Il convient en effet de se référer au chapitre X ("*Traitement de données à caractère personnel à des fins historiques, scientifiques ou statistiques*") du sous-titre 1 (les articles 99 à 104 inclus), du sous-titre 3 (les articles 132 à 137 inclus) et du sous-titre 4 (les articles 162 à 167 inclus) du titre III de la LPD qui ont prévu à cet égard un règlement propre pour une telle communication de données à caractère personnel. La responsabilité de cette communication repose ainsi sur les services respectifs en tant que responsable du traitement. De toute évidence, il n'est pas logique que le cadre juridique actuel ne prévoie pas ces possibilités pour les données policières qui sont généralement bien plus demandées dans le monde scientifique.

Une autre option éventuelle consiste à ce que le COC émette un avis contraignant dans lequel il lui appartiendrait d'évaluer la légalité (finalité, limitation de données, sécurité de l'information, etc.) et la proportionnalité de la communication de données policières au(x) chercheur(s). Cela s'inscrirait d'emblée dans le prolongement de la compétence du COC (et est similaire à celle-ci) prévue dans l'article 44/11/9, § 2 de la LFP abordé ci-avant. Dans ce cas, un arrêté royal n'est plus nécessaire.

III.2. Modifications de la loi du 7 décembre 1998 relative à la police intégrée

17. L'Organe de contrôle est très positif à l'égard de la création du Comité d'avis en charge de la stratégie en matière d'information (Comité Information et ICT). Il doit être en mesure d'apporter aide et conseils au responsable du traitement et aux sous-traitants de la police intégrée en ce qui concerne les nombreux thèmes, questions ou points de discussion souvent difficiles qui se présentent pour les différentes entités policières et leurs responsables. Il doit être en mesure d'agir en tant que premier intervenant pour le compte de la police afin de trouver des solutions et apporter des réponses pour ce qui se passe sur le terrain au sujet des thèmes vie privée, protection des données, gestion de l'information, technologies de l'information et sécurité de l'information, sans préjudice évidemment de leur propre responsabilité et de celle des délégués à la protection des données respectifs. Le COC ne peut en effet que constater qu'il reçoit déjà actuellement de très nombreuses questions qui devraient être traitées dans une première phase par le responsable du traitement lui-même. À l'avenir, ils pourront s'adresser au préalable à ce nouveau Comité Information et ICT qui devra également tenter de dégager des solutions et visions uniformes pour l'ensemble de la police intégrée.

Le projet souhaite confier au Comité Information et ICT une compétence particulière : un rapport annuel sur la mise en œuvre des règles de ventilation. Le COC salue cette mission, qui rejoint aussi ses remarques formulées ci-dessus au point 10 et qui s'inscrit dans le prolongement de la préoccupation du Gouvernement quant à l'exécution des règles d'effacement et d'archivage, telle qu'elle ressort de la notification au Conseil des ministres.

Dans le deuxième paragraphe, l'Organe de contrôle part du principe que, bien que cela ne ressorte pas explicitement de l'Exposé des motifs, au point c) toute une série de questions juridiques – ou du moins les plus essentielles ou les plus fondamentales – peuvent aussi être saisies. Ici aussi, le COC doit souvent répondre que l'Organe de contrôle n'a pas pour but (le COC n'est pas le conseiller juridique de l'ensemble de la police intégrée), ni forcément la capacité de réagir à toutes sortes de questions ou remarques ou d'émettre un avis. Ce type de questions doivent être abordées selon un système de cascade : en premier lieu, le responsable du traitement doit développer une réponse (avec son DPO) ; ensuite, on pourrait s'adresser au nouveau Comité Information et ICT et seulement en dernier lieu, à l'Organe de contrôle qui peut alors s'exprimer en connaissance de cause (il peut alors prendre connaissance de la vision du responsable du traitement, du DPO et/ou du Comité Information et ICT).

L'Organe de contrôle souhaite enfin être informé de tous les avis émis par le Comité Information et ICT. Pour être en mesure d'exercer ses missions d'autorité de contrôle de manière qualitative, il est évidemment primordial d'être et de rester informé de la vision, des initiatives et des points de vue de la police intégrée et de ses autorités de tutelle.

18. Le titre V de la LPI, actuellement abrogé, est rétabli avec une série de dispositions portant sur certaines modalités des traitements de données. Le projet d'article 144 de la LPI (article 30 de l'avant-projet) introduit l'obligation, pour chaque zone de police, le commissariat général, toute direction générale et direction de la police fédérale, de désigner un délégué à la protection des données (DPO) et exécute ainsi l'article 37 de la LPD et l'article 63 du RGPD et il impose une obligation similaire aux sous-traitants qui travaillent avec les responsables du traitement de la police.

Le COC demande qu'au 4^e paragraphe du projet d'article 144, l'avis du COC soit rendu obligatoire dans l'élaboration de l'arrêté d'exécution qui y est visé.

19. Le projet d'article 145, qui crée la base légale pour un registre électronique des traitements, ne précise pas s'il sera imposé obligatoirement à toutes les zones de police et entités de la police fédérale. Il semblerait que l'on puisse déduire implicitement de l'Exposé des motifs que le but est d'en faire une obligation. Pour le COC, il est préférable d'inscrire d'emblée l'obligation légale à l'article 145.

De nouveau, le COC demande que dans le projet d'article 145, l'avis de l'Organe de contrôle soit rendu obligatoire dans l'élaboration de l'arrêté d'exécution qui y est visé, lequel fixera la forme et les modalités du registre.

20. Le projet d'article 146 est une application de l'article 9.2 de la Directive Police et Justice. La disposition est toutefois très générale. L'Organe de contrôle propose de se référer à l'article 29 de la LPD : *"Conformément aux conditions de l'article 29 de la LPD, les responsables du traitement communiquent ..."*

21. Le projet d'article 147 (article 33 de l'avant-projet) prévoit aussi, pour les demandes d'accès dans les matières du RGPD où il est question d'un traitement de données qui avait été réalisé initialement par la police en application du titre 2 de la LPD, un accès indirect dans l'exercice des droits via l'Organe de contrôle. Cet article se situe dans le même esprit que l'article 14, § 6 de la LPD où le COC a tout autant une responsabilité dans les demandes d'exercice des droits de la personne concernée auprès

d'une autorité qui relève du titre 1 de la LPD/du RGPD et qui concernent des informations qui ont été traitées initialement par les services de police (dans le cadre de leurs missions opérationnelles). Le 2^e alinéa du 1^e paragraphe semble être superflu et faire double emploi avec l'article 14, § 2 de la LPD.

En l'espèce, il n'est pas précisé quelle information le COC peut/doit communiquer dans ce cas à la personne concernée. À l'article 14, § 6, 2^e alinéa de la LPD évoqué ci-avant, on affirme que lorsque l'APD a été saisie par la personne concernée, après réception de la réponse de l'Organe de contrôle, l'APD informe la personne concernée *"selon les modalités légales prévues"*. On ne précise pas quelles sont ces modalités. Quoi qu'il en soit, à défaut de description plus détaillée, le COC aura la responsabilité d'évaluer quelles informations peuvent être communiquées. C'est par ailleurs la solution que préfère l'Organe de contrôle. La seule mention du fait *"qu'il a été procédé aux vérifications nécessaires"*, comme prévu par le titre 2 (article 42 de la LPD) génère très souvent une incompréhension totale chez la personne concernée.

De manière plus générale, il convient d'ailleurs de remarquer que l'article 41 de la LPD n'instaure pas d'emblée un système d'accès indirect, même si on en est parfois manifestement convaincu sur le terrain. Cet article dispose en effet que : *"la loi, le décret ou l'ordonnance, peut prévoir que les droits de la personne concernée sont exercés par l'intermédiaire de l'autorité de contrôle compétente"*. Bien que cette disposition puisse être lue dans le sens où, par "loi", on viserait aussi la LPD elle-même, il ne semble pas que telle était l'intention du législateur. Dans l'Exposé des motifs de la LPD, l'intention de l'article 41 de la LPD est en effet motivée comme suit : *"Il s'agit de laisser le système de l'accès indirect une option pour les autorités qui le souhaitent. Il est également prévu que lorsqu'il est fait application de l'accès indirect, la demande se fait via l'autorité de contrôle compétente."*¹⁷ Le fait que cet article 42 dispose que la demande doit être adressée au COC est la simple mise en œuvre de l'article 17, 1^e alinéa de la Directive Police et Justice. Il convient donc de mettre fin à cette imprécision dans la LFP.

22. Enfin, l'Organe de contrôle comprend parfaitement que les dispositions ambitieuses concernant la journalisation ne puissent pas toutes entrer en vigueur immédiatement. Il s'agit de la journalisation concernant les traitements dans la BNG, dans les archives de la BNG, dans les banques de données de base et dans les banques de données particulières. Le renvoi, à l'article 34 de l'avant-projet, à l'article 279 de la LPD est probablement une erreur ; on vise incontestablement l'article 284 de la LPD. En ce qui concerne toutefois les traitements dans la BNG, l'Organe de contrôle ne voit aucune bonne raison de ne pas faire entrer en vigueur immédiatement la conservation des fichiers de journalisation pendant 30 ans. Les fichiers de journalisation de la BNG sont d'ores et déjà conservés de sorte que l'on ne comprend pas pourquoi un report à 2023 serait encore nécessaire.

¹⁷ Doc. Parl. Chambre 2017-2018, 54-3126/001, 84. Marquage propre.

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

demande

- **de donner suite aux remarques reprises aux points 3 à 6 inclus, 8, 9, 12 à 16 inclus et 18 à 21 inclus**
- **de tenir compte des remarques susmentionnées aux points 10, 11, 17 et 22**

Avis approuvé par l'Organe de contrôle de l'information policière le 12 décembre 2018.

Pour l'Organe de contrôle,

le Président,

(sé.) Philippe ARNOULD

p.o. Frank Schuermans

Membre-conseiller

DE RAAD VAN BURGEMEESTERS

De Raad van Burgemeesters
Secretariaat

Waterloolaan 76
B- 1000 Brussel
Tel. 02 557 33 90
Fax 02 557 33 97
vclp@ibz.fgov.be

Uw bericht van 27-12-2018
Uw kenmerk SAT/
Ons kenmerk RIO - 2019/

De Heer Geens
Minister van Justitie

Waterloolaan, 115
1000 Brussel

Brussel	2019-01-11
Dossierbeheerder	E Wauters
Telefoon	02 557 33 91
Fax	02 557 33 97
E-mail	vclp@ibz.fgov.be

Onderwerp: Voorontwerp van wet betreffende het politionele informatiebeheer en tot wijziging van de wet op het politieambt en de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus

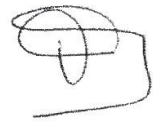
Geachte Heer Minister,

De burgemeesters van de Raad hebben kennisgenomen van het voorontwerp van wet betreffende het politionele informatiebeheer en tot wijziging van de wet op het politieambt en de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus.

De burgemeesters hebben enkele bemerkingen geformuleerd, waarvoor we verwijzen naar de bijlage.

Met de meeste hoogachting,


Patrick De Munter
Vast Secretaris


Marnic De Meulemeester
Burgemeester- Voorzitter

Bijlage : bemerkingen burgemeesters

Bijlage : verzamelde bemerkingen

Wij hebben nota genomen over uw vraag voor advies van het voorontwerp van wet betreffende het politionele informatiebeheer en tot wijziging van de wet op het politieambt en de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus.

Het informatiebeheer is voor de veiligheidsketen een belangrijk onderwerp. Politie moet in staat zijn om gegevens over hun optreden te bewaren en deze te delen met gerechtelijke en bestuurlijke overheden. Dit met respect voor de elementaire rechten van privacy. De omzetting van de nieuwe Europese wetgeving (Richtlijn 2016/680 en Verordening 2016/679) is uiteraard zeer belangrijk. Deze dient dringend te worden afgewerkt. Zie namelijk de reeds verstreken omzettingstermijn van 6 mei 2018 voor Richtlijn 2016/680 (artikel 63.1).

Er dient dringend een kader te komen voor de het register, DPO en de categorieën van persoonsgegevens die kunnen worden bewaard. Daarbij is ook gedacht aan de gegevens van bestuurlijke politie.

Een bestuurlijke overheid moet in sommige gevallen in staat kunnen zijn om informatie te ontvangen voor politieactiviteiten bij demonstraties, belangrijke sportevenementen en rellen. Dit kan in de toekomst misschien nog verder worden uitgewerkt.

Wel ontbreekt een exclusieve categorie in het voorontwerp van persoonsgegevens naar aanleiding van feiten die enkel met (exclusieve) administratieve sancties kunnen worden gesanctioneerd.

Desondanks vragen wij verdere behandeling van dit dossier zodat deze Europese regelgeving correct kan worden toegepast.

Op zich is het een goed initiatief om een uniek register te voorzien i.p.v. elke zone of dienst dit te laten ontwerpen maar hieronder staan een aantal bezorgdheden van experts in de materie:

- verwerkingsregister als middel voor informatieveiligheid *versus* verwerkingsregister type RegPol om te voldoen aan wettelijke bepaling: huidig opzet is een poging om te voldoen aan de wettelijke verplichtingen maar hierdoor weinig dienstig voor risicoanalyse van de processen binnen de GPI noch voor andere opdrachten van de data protection officer;
- RegPol omvat geen dienstige functionaliteiten inzake meldingsplicht bij datalekken noch een "Incident management register" (en bijhorende risicoanalyse);
- Er is in RegPol geen politioneel herkenbare structuur. Bijvoorbeeld een onderscheid naar gegevens die:
 - onder Titel I en Titel II van de wet 30/07/18 vallen
 - onder opdrachten van bestuurlijke en gerechtelijke politie

Annexe : recueil de remarques

Nous avons pris note de votre demande d'avis concernant l'avant-projet de loi relatif à la gestion de l'information policière et modifiant la loi sur la fonction de police et la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux.

La gestion de l'information est une question importante pour la chaîne de sécurité. La police doit être en mesure de conserver des données concernant leurs interventions et de les partager avec des autorités judiciaires et administratives et ce, dans le respect des droits élémentaires de la vie privée. La transposition de la nouvelle législation européenne (Directive 2016/680 et Règlement 2016/679) est évidemment très importante. Cette transposition doit être finalisée au plus vite. Voir en effet le délai de transposition déjà expiré du 6 mai 2018 pour la Directive 2016/680 (article 63.1).

Il convient d'établir d'urgence un cadre pour le registre, le DPO et les catégories de données à caractère personnel qui peuvent être conservées. Les données de police administrative ont également été envisagées.

Une autorité administrative doit, dans certains cas, être en mesure de recevoir des informations relatives à des activités policières lors de manifestations, de grands événements sportifs et d'émeutes. Ce point pourrait à l'avenir être davantage développé.

Il manque toutefois dans l'avant-projet une catégorie exclusive de données à caractère personnel suite à des faits ne pouvant être sanctionnés que par des sanctions administratives (exclusives).

Nous demandons néanmoins à ce que ce dossier aboutisse afin de pouvoir appliquer correctement cette réglementation européenne.

Il s'agit en soi d'une bonne initiative de prévoir un registre unique au lieu de demander à chaque zone ou service de conceptualiser son propre registre. Néanmoins, vous trouverez ci-dessous un certain nombre de préoccupations exprimées par des experts en la matière :

- Le registre de traitement comme moyen de garantir la sécurité de l'information vs. le registre de traitement type RegPol pour se conformer à la disposition légale : la solution actuellement proposée tente de répondre aux obligations légales mais elle s'avère peu utile, tant dans le cadre de l'analyse de risques des processus existant au sein de la GPI que pour l'exercice d'autres missions du délégué à la protection des données ;
- Le RegPol ne prévoit pas de fonctionnalités utiles concernant l'obligation de notification en cas de fuites de données, ni aucun registre de gestion des incidents (et analyse de risques y afférente) ;
- Le RegPol est dépourvu d'une structure policière reconnaissable. Par exemple, une distinction entre les données relevant :

- o des Titres I et II de la loi du 30 juillet 1978 ;

- o des missions de police administrative et judiciaire.

LE CONSEIL DES BOURGMESTRES

Le Conseil des Bourgmestres
Secrétariat
Boulevard de Waterloo 76
1000 Bruxelles
Tél. 02 557 33 90

Monsieur Geens
Ministre de la Justice
Boulevard de Waterloo 115
1000 Bruxelles

Votre courrier du
Vos références
Nos références

Bruxelles
Gestionnaire de dossier
Téléphone
Fax
E-mail

Objet : Avant-projet de loi relatif à la gestion de l'information policière et modifiant la loi sur la fonction de police et la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux

Monsieur le Ministre,

Les bourgmestres du Conseil ont pris connaissance de l'avant-projet de loi relatif à la gestion de l'information policière et modifiant la loi sur la fonction de police et la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux.

Les bourgmestres ont formulé quelques remarques, lesquelles ont été jointes en annexe.

Je vous prie d'agréer, Monsieur le Ministre, l'expression de nos salutations distinguées,

Secrétaire permanent

Bourgmestre-Président

Annexe : remarques des bourgmestres

Van: De La Serna Ignacio

Verzonden: dinsdag 12 maart 2019 19:50

Aan: Godin Samuelle <Samuelle.Godin@just.fgov.be>

CC: De Valkeneer Christian <Christian.DeValkeneer@just.fgov.be>; Delmulle Johan <Johan.Delmulle@just.fgov.be>; Vandenbruwaene Patrick <Patrick.Vandenbruwaene@just.fgov.be>; Dernicourt Erwin <Erwin.Dernicourt@just.fgov.be>; Van Leeuw Frédéric <Frederic.VanLeeuw@just.fgov.be>; Godart Ingrid <Ingrid.Godart@just.fgov.be>; De Biolley Serge <Serge.DeBiolley@just.fgov.be>

Onderwerp: Avis Collège PG - Loi sur la gestion de l'information policière

Bonsoir Madame,

Le Collège a pu très brièvement examiner l'avant-projet de loi sur la gestion de l'information policière.

Au nom du Collège PG, je peux officiellement vous faire part de notre avis globalement favorable en ce qui concerne cet avant-projet à l'exception du point suivant.

En effet, le Collège émet de **sérieuses réserves** quant à un accès direct à la BNG pour les services de renseignement (art. 44/11/12) ainsi qu'en ce qui concerne la communication des données à caractère personnel et les informations (art. 44/11/8bis) sans réciprocité pour les services de police d'avoir un accès aux banques de données des services de renseignement.

Le Collège constate que le COC a émis également des réserves similaires.

Le Collège souhaite vivement pouvoir être associé à la détermination des modalités de cette réciprocité.

Enfin, le Collège estime que cette question fait également l'objet de la discussion portant sur la banque carrefour de sécurité. Le chef de cabinet adjoint du Ministre de la Justice, Serge de Biolley sera d'ailleurs invité la semaine prochaine pour une discussion sur ce sujet.

Bien à vous,

Pour le Collège PG,

Ignacio de la Serna

Procureur général

Tel : 065/37.90.11

Ignacio.delaserna@just.fgov.be

www.ministerepublic.be