SERVICE PUBLIC FEDERAL JUSTICE ET MINISTERE DE LA DEFENSE

[C − 2019/15040]

2 OCTOBRE 2019. — Arrêté royal modifiant l'arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'arrêté royal du 3 juillet 2016 portant exécution de l'article 21 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

RAPPORT AU ROI

Sire,

La nouvelle loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (ci-après nommée la « loi du 30 juillet 2018 ») a désigné le Comité permanent R comme autorité de protection des données pour les traitements de données à caractère personnel effectués par les services de renseignement et a introduit quelques autres changements qui nécessitent certaines adaptations de l'arrêté royal du 12 octobre 2010 et de l'arrêté royal du 3 juillet 2016 portant exécution de l'article 21 de la loi du 30 novembre 1998.

Par ailleurs, la loi du 30 mars 2017 a modifié la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (ci-après nommée la « loi du 30 novembre 1998 ») afin de solutionner les problèmes opérationnels rencontrés, tout en améliorant et clarifiant la loi du 30 novembre 1998.

La loi précitée du 30 mars 2017 a notamment inséré une nouvelle section intitulée « Mesures de protection et d'appui » dans laquelle se retrouve l'ancien article 13/1 scindé en deux : article 13/1 : les infractions – article 13/2 : les faux noms.

A l'article 13/2, est ajoutée l'utilisation d'une identité ou qualité fictive. Cette utilisation est retirée de la méthode exceptionnelle de front store pour en faire une mesure de protection et d'appui autonome.

Est inséré un article 13/3 permettant la création d'une personne morale et son utilisation pour d'autres raisons que la collecte, et ce, comme mesure de protection et d'appui et non plus comme méthode exceptionnelle.

Il convient de déterminer les modalités d'exécution de ces mesures de protection et d'appui et de compléter celles qui sont déjà prévues dans l'arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (ci-après nommé « l'arrêté royal du 12 octobre 2010 »).

La loi du 30 mars 2017 modifie en outre quelques éléments de procédure dans l'ensemble de la loi du 30 novembre 1998, ce qui justifie également l'adaptation de l'arrêté royal du 12 octobre 2010.

Enfin, la loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière a inséré un nouvel article 16/4 dans la loi du 30 novembre 1998, permettant aux services de renseignement d'avoir accès aux informations et données à caractère personnel qui sont collectées au moyen de caméras utilisées par les services de police. Les modalités d'un tel accès doivent être déterminées par arrêté royal.

Commentaire des articles

CHAPITRE I. — *Modification de l'arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité*

Article 1

L'article 1 du présent projet remplace la référence à la loi du 8 décembre 1992 dans l'article 1er, 3° de l'arrêté royal du 12 octobre 2010, par une référence à la loi du 30 juillet 2018, qui abroge la précédente.

Article 2

L'article 2 vise à adapter l'intitulé du chapitre II de l'arrêté royal du 12 octobre 2010 pour viser l'ensemble des mesures de protection et d'appui, et plus uniquement le faux nom.

FEDERALE OVERHEIDSDIENST JUSTITIE EN MINISTERIE VAN LANDSVERDEDIGING

[C − 2019/15040]

2 OKTOBER 2019. — Koninklijk besluit tot wijziging van het koninklijk besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en het koninklijk besluit van 3 juli 2016 houdende uitvoering van artikel 21 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst

VERSLAG AAN DE KONING

Sire,

De nieuwe wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (hierna de "wet van 30 juli 2018" genoemd) heeft het Vast Comité I als gegevensbeschermingsautoriteit voor de verwerking van persoonsgegevens door de inlichtingendiensten aangewezen en heeft enkele andere wijzigingen ingevoerd die bepaalde aanpassingen aan het koninklijk besluit van 12 oktober 2010 en het koninklijk besluit van 3 juli 2016 houdende uitvoering van artikel 21 van de wet van 30 november 1998 vereisen.

De wet van 30 maart 2017 heeft bovendien de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (hierna de "wet van 30 november 1998" genoemd) gewijzigd om de operationele problemen die zich voorgedaan hebben, op te lossen en daarbij de wet van 30 november 1998 te verbeteren en verduidelijken.

De voornoemde wet van 30 maart 2017 heeft met name een nieuwe afdeling ingevoegd luidende "De beschermings- en ondersteuningsmaatregelen" waarin het oude artikel 31/1 in twee gesplitst wordt: artikel 13/1: strafbare feiten/artikel 13/2 – valse namen.

In artikel 13/2 wordt het gebruik van een fictieve identiteit of hoedanigheid toegevoegd. Dit gebruik wordt uit de uitzonderlijke methode van de frontstore gehaald om er een autonome beschermings- en ondersteuningsmaatregel van te maken.

Er wordt een artikel 13/3 ingevoegd dat de oprichting van een rechtspersoon toelaat en het gebruik ervan voor andere doeleinden dan de inzameling en dit als beschermings- en ondersteuningsmaatregel en niet meer als uitzonderlijke methode.

De nadere regels voor de uitvoering van deze beschermings- en ondersteuningsmaatregelen moeten worden vastgesteld en degene die reeds voorzien zijn in het koninklijk besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (hierna "het koninklijk besluit van 12 oktober 2010" genoemd) moeten worden aangevuld.

De wet van 30 maart 2017 wijzigt bovendien enkele elementen van de procedure in de volledige wet van 30 november 1998, wat eveneens de aanpassing van het koninklijk besluit van 12 oktober 2010 rechtvaardigt.

Ten slotte heeft 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 een nieuw artikel 16/4 in de wet van 30 november 1998 ingevoegd dat de inlichtingendiensten toelaat toegang te hebben tot informatie en persoonsgegevens die verzameld worden door middel van door de politiediensten gebruikte camera's. De nadere regels voor een dergelijke toegang moeten bij koninklijk besluit worden bepaald.

Toelichting van de artikelen

HOOFDSTUK I. — *Wijziging van het koninklijk besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten*

Artikel 1

Artikel 1 van deze wet vervangt de verwijzing naar de wet van 8 december 1992 in artikel 1, 3° van het koninklijk besluit van 12 oktober 2010 door een verwijzing naar de wet van 30 juli 2018 die de voorgaande afschaft.

Artikel 2

Artikel 2 beoogt het opschrift van hoofdstuk II van het koninklijk besluit van 12 oktober 2010 aan te passen teneinde betrekking te hebben op alle beschermings- en ondersteuningsmaatregelen en niet enkel op de valse naam.

Article 3

L'article 2 de l'arrêté royal du 12 octobre 2010 détermine les modalités d'utilisation d'un faux nom. Le présent projet vise à le compléter avec les modalités d'utilisation d'une identité ou d'une qualité fictive qui se trouvent désormais dans le même article (art. 13/2).

Les mêmes modalités sont fixées pour l'utilisation d'une identité ou d'une qualité fictive que pour l'utilisation d'un faux nom. Ces modalités sont d'ailleurs reprises de l'article 6 de l'arrêté royal du 12 octobre 2010. Une exigence supplémentaire est prévue : tenir le dirigeant du service, ou la personne qu'il désigne à cet effet, au courant du déroulement de cette utilisation. Cela se fait par écrit tous les deux mois. Ce délai est calqué sur le délai fixé à l'article 18/13 pour l'utilisation d'une personne morale comme méthode de collecte : cela se justifie car il s'agit d'une utilisation qui peut s'étendre sur une longue période sans nécessairement être activée fréquemment. Une mise au courant à intervalle très court ne se justifie donc pas.

Un alinéa 4 est ajouté pour prévoir un délai de conservation du journal de bord, pour ne pas entraver un contrôle a posteriori. Pour répondre au point 4 de l'avis du Comité permanent R, le délai de conservation a été porté à dix ans, au lieu de cinq. Comme le remarque le Comité permanent R, un délai de dix ans est déjà prévu dans l'arrêté royal du 12 octobre 2010 pour les logs dans les banques de données du secteur public et pour les journaux de bord des identités fictives (actuel article 6).

En s'alignant sur ce délai, on obtient en effet l'harmonisation des délais de conservation.

Article 4

L'article 4 du présent projet vise à insérer un nouvel article 2/1 fixant les modalités de création et d'utilisation d'une personne morale en exécution de l'article 13/3 de la loi du 30 novembre 1998. Celles-ci sont similaires à celles prévues pour l'utilisation d'un faux nom, d'une identité ou d'une qualité fictive.

L'article 13/3, § 1er de la loi du 30 novembre 1998 autorise le Roi à prévoir la possibilité de déroger aux dispositions légales applicables en cas de dissolution et de liquidation d'une personne morale. Cette possibilité est mise en œuvre à l'article 2/1 de l'arrêté royal du 12 octobre 2010. Une dérogation n'est autorisée que lorsque cela se justifie pour des besoins opérationnels ou de discrétion. La décision est prise par le dirigeant du service, elle est écrite, motivée et notifiée au Comité permanent R.

En réaction au point 5 de l'avis du Comité permanent R, des modalités de mise en œuvre de la possibilité de créer une personne morale ont été ajoutées et il a été décidé de ne pas exécuter la dernière phrase du § 1er de l'article 13/3 de la loi du 30 novembre 1998 pour le moment. En effet, vu la complexité des règles de dissolution et de liquidation, le nombre de personnes morales différentes et la toute nouvelle législation en matière de sociétés et associations, cette exécution est reportée afin de procéder à une analyse plus approfondie.

Article 5

Cet article modifie l'intitulé du chapitre III pour viser l'ensemble des banques de données externes.

En effet, comme cela ressort des recommandations de la commission d'enquête parlementaire sur les attentats de Bruxelles, il faut développer une meilleure connexion des services de renseignement et de sécurité aux données utiles à l'exécution de leurs missions. Ces données peuvent être en possession tant du secteur public que du secteur privé. La présente modification de l'arrêté royal n'octroie pas d'accès à une banque de données externe, il détermine seulement les modalités à appliquer lorsqu'un tel accès existe par ou en vertu d'une loi, ou avec le consentement du responsable du traitement de la banque de données.

Article 6

L'article 6 adapte l'article 3 de l'arrêté royal du 12 octobre 2010 afin de fixer les modalités d'accès à toute banque de données auxquelles les services de renseignement ont ou auront accès, par ou en vertu d'une loi spécifique ou, sur base des articles 14 (données du secteur public) et 16 (données du secteur privé) de la loi organique, avec le consentement du responsable du traitement de la banque de données.

Cet article exécute notamment les articles 14, 16/2 et 16/4 de la loi du 30 novembre 1998.

Artikel 3

Artikel 2 van het koninklijk besluit van 12 oktober 2010 bepaalt de nadere regels voor het gebruik van een valse naam. Dit ontwerp beoogt deze aan te vullen met de nadere regels voor het gebruik van een fictieve identiteit of hoedanigheid die zich voortaan in hetzelfde artikel bevinden (art. 13/2).

Dezelfde nadere regels worden zowel voor het gebruik van een fictieve identiteit of hoedanigheid als voor het gebruik van een valse naam vastgelegd. Deze nadere regels worden bovendien in artikel 6 van het koninklijk besluit van 12 oktober 2010 vermeld. Een bijkomende vereiste wordt voorzien: het diensthoofd, of de persoon die hij hiertoe aanstelt, op de hoogte houden tijdens het verloop van dit gebruik. Dit gebeurt schriftelijk om de twee maanden. Deze termijn is dezelfde als de termijn vastgelegd in artikel 18/13 voor het gebruik van een rechtspersoon als inlichtingenmethode: dit is gerechtvaardigd omdat het gaat om een gebruik dat een lange periode kan beslaan, zonder noodzakelijk vaak aangewend te worden. Het is dus niet gerechtvaardigd om met zeer korte tussenpozen te informeren.

Een lid 4 wordt toegevoegd om een termijn te voorzien voor het bewaren van het logboek om een controle a posteriori niet te belemmeren. Om te beantwoorden aan punt 4 van het advies van het Vast Comité I werd de bewaartermijn op tien jaar, in plaats van vijf, gebracht. Zoals opgemerkt door het Vast Comité I, wordt een termijn van tien jaar reeds voorzien in het koninklijk besluit van 12 oktober 2010 voor de logs van de gegevensbanken van de publieke sector en voor de logboeken van de fictieve identiteiten (huidig artikel 6).

Door zich op deze termijn af te stemmen verkrijgt men inderdaad de harmonisering van bewaartermijnen.

Artikel 4

Artikel 4 van dit ontwerp beoogt een nieuw artikel 2/1 in te voegen dat de nadere regels voor de oprichting en het gebruik van een rechtspersoon in uitvoering van artikel 13/3 van de wet van 30 november 1998 vastlegt. Deze zijn vergelijkbaar met de regels voorzien voor het gebruik van een valse naam, een fictieve identiteit of hoedanigheid.

Artikel 13/3, § 1 van de wet van 30 november 1998 machtigt de Koning om de mogelijkheid te voorzien af te wijken van de wettelijke bepalingen die van toepassing zijn in geval van ontbinding en vereffening van een rechtspersoon. Hieraan wordt uitvoering verleend door artikel 2/1 van het koninklijk besluit van 12 oktober 2010. Een afwijking is enkel toegestaan wanneer dit voor operationele doeleinden of omwille van discretie gerechtvaardigd is. De beslissing wordt door het diensthoofd genomen, zij wordt schriftelijk meegedeeld, met redenen omkleed en ter kennis gebracht van het Vast Comité I.

In reactie op punt 5 van het advies van het Vast Comité I werden nadere regels toegevoegd voor de aanwending van de mogelijkheid om een rechtspersoon op te richten en werd beslist om de laatste zin van de eerste paragraaf van artikel 13/3 van de wet van 30 november 1998 voorlopig niet uit te voeren. Inderdaad, gezien de ingewikkelde regels voor ontbinding en vereffening, het aantal verschillende rechtspersonen en de volledig nieuwe wetgeving inzake vennootschappen en verenigingen wordt deze uitvoering uitgesteld om een diepgaandere analyse uit te voeren.

Artikel 5

Dit artikel wijzigt het opschrift van hoofdstuk III door de woorden "van de openbare sector" te schrappen.

Zoals blijkt uit de aanbevelingen van de parlementaire onderzoekscommissie naar de aanslagen in Brussel moet er een betere verbinding tot stand gebracht worden van de inlichtingen- en veiligheidsdiensten met de gegevens die nuttig zijn voor de uitvoering van hun opdrachten. Deze gegevens kunnen in het bezit zijn van zowel de publieke als de private sector. Deze wijziging van het koninklijk besluit verleent geen toegang tot een externe gegevensbank, het bepaalt enkel de nadere regels die moeten worden toegepast wanneer een dergelijke toegang bestaat door of krachtens een wet of met de toestemming van de verwerkingsverantwoordelijke van de gegevensbank.

Artikel 6

Artikel 6 wijzigt artikel 3 van het koninklijk besluit van 12 oktober 2010 om de toegangsbepalingen vast te leggen voor elke gegevensbank waartoe de inlichtingen- en veiligheidsdiensten toegang hebben of zullen hebben, door of krachtens een specifieke wet, of, op basis van artikelen 14 (gegevens van de openbare sector) of 16 (gegevens van de private sector), met de toestemming van de verwerkingsverantwoordelijke van de gegevensbank.

Dit artikel voert meer bepaald de artikelen 14, 16/2 en 16/4 van de wet van 30 november 1998 uit.

Dans son avis (point 9), le Comité permanent R souligne qu'un accès direct à des banques de données ne peut être utilisé pour contourner des procédures légales qui prévoient un contrôle spécifique, par exemple, lorsqu'il s'agit de méthodes spécifiques ou exceptionnelles. Dans ce cas, aucun accès ne pourrait être organisé. Le gouvernement tient à remarquer qu'il n'est en effet pas question de contourner des procédures légales en organisant un accès à des banques de données. Ce qui ne signifie pour autant pas qu'un accès direct ne puisse pas être organisé pour exécuter une méthode spécifique ou exceptionnelle. Il faut tout simplement respecter la procédure prévue pour la mise en œuvre d'une méthode spécifique ou exceptionnelle avant d'utiliser concrètement l'accès à la banque de données concernée. C'est ainsi le cas dans le cadre des articles 18/4 et 18/11 de la loi du 30 novembre 1998, lorsqu'il s'agit d'une observation en temps réel, avec recours aux données collectées par des caméras utilisées par la police pour lesquelles un accès direct des services de renseignement est autorisé.

La présente disposition fixe les principes de base à appliquer quand un accès direct à une banque de données externe est implémenté.

Dans le point 10 de son avis, le Comité permanent R recommande de définir les termes 'accès direct' et 'interrogation directe'. Il ne paraît pas approprié d'ajouter la définition d''accès direct' dans le texte-même du projet d'arrêté royal, dès lors que ces termes existent dans la loi du 30 novembre 1998 (article 16/4).

Par 'accès direct', on entend tous les accès aux données contenues dans des banques de données externes, sans l'intermédiaire d'un tiers pour leur consultation. Ces termes étaient déjà présents dans l'article 3 de l'arrêté royal du 12 octobre 2010 modifié par le présent projet. Comme indiqué plus haut, ils apparaissent dorénavant aussi dans l'article 16/4 de la loi du 30 novembre 1998. Par contre, les termes 'interrogation directe' ont été supprimés du projet dès lors qu'ils sont propres à la loi sur la fonction de police. Il n'y a dès lors pas lieu de les définir dans ce cadre, ni de les ajouter dans d'autres dispositions, comme le suggérait notamment le point 18 de l'avis du Comité permanent R.

A l'instar de ce que prévoit le paragraphe 2 – une situation où l'accès direct est impossible, ce qui renvoie tant à une impossibilité technique, qu'à une impossibilité temporaire ou encore à un accès non encore installé (point 18 de l'avis du Comité permanent *R)*, quand un accès direct n'est pas assuré, l'alinéa 2 du paragraphe 1er précise que l'accès direct peut être pallié par la fourniture des fichiers de données de la banque de données externe audit service de renseignement, si les capacités d'enregistrement dudit service de renseignement le permettent. Il s'agit d'une faculté concertée entre les deux parties permettant de s'adapter en fonction des capacités technologiques de chaque banque de données, l'objectif étant d'atteindre le meilleur flux possible. A titre d'illustration, la DIV préfère la communication de fichiers vers un destinataire plutôt qu'une consultation dans sa banque de données, afin d'éviter une lenteur des traitements de ses propres services dans la banque de données, due à une surcharge du système.

Dans le point 14 de son avis, le Comité permanent R s'interroge sur l'étendue de cette fourniture de fichiers de données contenus dans une banque de données externe. Comme le suggère le Comité permanent R, cela couvre en effet un « ensemble de fichiers ou de larges pans d'une banque de données ». La question de proportionnalité et de finalité ne diffère en rien dans ce processus à celle qui existe dans le cadre d'un accès direct. Les mêmes contrôles seront exercés sur les logs dans un système comme dans l'autre. Quant à la préoccupation du Comité permanent R portant sur l'exactitude des données par rapport à leur éventuelle mise à jour dans la banque de données dont on a fourni un ensemble de fichiers, il y a lieu de préciser qu'un tel système de fourniture sera toujours combiné à la transmission des actualisations des données fournies. Parallèlement, les agents qui ont accès aux données fournies seront informés des modalités liées à la mise à jour de ces données (message, système d'alerte, ...). Lors de la communication à des tiers d'informations issues de copies et lors de la prise de décisions produisant des effets juridiques pour la personne concernée, les agents ont une obligation de moyen de vérifier, au moment de la rédaction de leur document, que les données traitées correspondent à leur dernière mise à jour disponible.

In zijn advies (punt 9) benadrukt het Vast Comité I dat een rechtstreekse toegang tot gegevensbanken niet gebruikt mag worden om wettelijke procedures die voorzien in een specifiek toezicht te omzeilen, bijvoorbeeld wanneer het gaat om specifieke of uitzonderlijke methoden. In dat geval mag geen enkele toegang worden georganiseerd. De regering wil hierbij opmerken dat de wettelijke procedures geenszins omzeild mogen worden bij de organisatie van toegang tot gegevensbanken. Dit betekent daarom niet dat een rechtstreekse toegang niet georganiseerd kan worden om een specifieke of uitzonderlijke methode uit te voeren. De procedure voorzien voor het gebruik van een specifieke of uitzonderlijke methode moet gewoon nageleefd worden vooraleer de toegang tot de betrokken gegevensbank concreet te gebruiken. Dit is aldus het geval in het kader van artikelen 18/4 en 18/11 van de wet van 30 november 1998 wanneer het gaat om een realtime-observatie, met gebruik van gegevens verzameld door camera's die door de politie gebruikt worden waarvoor een rechtstreekse toegang voor de inlichtingendiensten is toegestaan.

De voorliggende bepaling legt de toe te passen basisprincipes vast wanneer een rechtstreekse toegang tot een externe gegevensbank wordt geïmplementeerd.

In punt 10 van zijn advies raadt het Vast Comité I aan om de termen 'rechtstreekse toegang' en 'rechtstreekse bevraging' te definiëren. Het lijkt niet aangewezen om de definitie van 'rechtstreekse toegang' toe te voegen in de tekst van het ontwerp van koninklijk besluit, aangezien deze termen reeds voorkomen in de wet van 30 november 1998 (artikel 16/4).

Onder 'rechtstreekse toegang' wordt elke toegang tot gegevens in externe gegevensbanken zonder tussenkomst van een derde voor hun raadpleging verstaan. Deze termen kwamen reeds voor in artikel 3 van het koninklijk besluit van 12 oktober 2010 dat door dit ontwerp gewijzigd wordt. Zoals hierboven vermeld, komen ze van nu af aan ook voor in artikel 16/4 van de wet van 30 november 1998. Daarentegen werden de termen 'rechtstreekse bevraging' uit het ontwerp geschrapt, aangezien ze specifiek zijn aan de wet op het politieambt. Deze termen dienen bijgevolg in dit kader niet gedefinieerd noch in andere bepalingen toegevoegd te worden, zoals met name in punt 18 van het advies van het Vast Comité I voorgesteld werd.

Net als wat paragraaf 2 voorziet – een situatie waarin de directe toegang onmogelijk is, wat zowel kan wijzen op een technische onmogelijkheid als op een tijdelijke onmogelijkheid of op een nog niet geïnstalleerde toegang (punt 18 van het advies van het Vast Comité *I)*, verduidelijkt lid 2 van de eerste paragraaf dat, wanneer een rechtstreekse toegang niet wordt verzekerd, de rechtstreekse toegang kan afgezwakt worden tot het verstrekken van gegevensbestanden van de gegevensbank die extern is aan de betrokken inlichtingen- en veiligheidsdienst, indien de opslagcapaciteit van de betrokken inlichtingen- en veiligheidsdienst dit toestaat. Het gaat om een mogelijkheid waarover overleg is gepleegd tussen beide partijen die het mogelijk maakt zich aan te passen op grond van de technologische capaciteiten van elke gegevensbank, waarbij het de bedoeling is tot een zo goed mogelijke stroom te komen. Ter illustratie: de DIV geeft veeleer de voorkeur aan de mededeling van bestanden aan een ontvanger dan aan een raadpleging van zijn gegevensbank om te voorkomen dat de verwerkingen van zijn eigen diensten in de gegevensbank traag verlopen door een overbelasting van het systeem.

In punt 14 van zijn advies vraagt het Vast Comité I zich af wat de omvang is van dit verstrekken van gegevensbestanden van externe gegevensbanken. Zoals het Vast Comité I aangeeft, dekt dit inderdaad "een geheel van gegevensbestanden of grote delen van een gegevensbank". De kwestie van proportionaliteit en doeleinde is in dit proces precies dezelfde als degene in het kader van een rechtstreekse toegang. Dezelfde controles worden uitgevoerd op de logs in beide systemen. Wat de bezorgdheid van het Vast Comité I betreft inzake de nauwkeurigheid van de gegevens met betrekking tot hun eventuele bijwerking in de gegevensbank waaruit een geheel van gegevensbestanden werd verstrekt, dient verduidelijkt te worden dat een dergelijk verstrekkingssysteem altijd gepaard gaat met de overdracht van de bijwerkingen van de verstrekte gegevens. Gelijktijdig zullen de agenten die toegang hebben tot de verstrekte gegevens geïnformeerd worden over de modaliteiten die verbonden zijn aan de update van deze gegevens (bericht, verwittiging, ...). Bij het vrijgeven van informatie aan derden en bij het nemen van beslissingen die juridische effecten genereren voor de betrokken persoon, hebben de agenten een inspanningsverbintenis om, op het moment van het opstellen van hun document, te verifiëren dat de verwerkte gegevens overeenkomen met de laatst beschikbare update.

En application de l'article 95 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, le Comité permanent R est désigné comme autorité de protection de données pour les services de renseignement. Les mots « Commission de la protection de la vie privée » sont donc remplacés, en application de l'article 253 de la loi précitée du 30 juillet 2018, par les mots « Comité permanent R ».

L'article 6 du présent projet insère aussi de nouveaux alinéas portant sur la journalisation des traitements.

Tous les traitements dans une banque de données doivent être enregistrés. Ceux des services de renseignement ne peuvent pas être visibles par tous ceux qui ont accès à la banque de données, raison pour laquelle des mesures de sécurité leur seront appliquées.

Le projet prévoit que ces mesures sont mises à la disposition du Comité permanent R, de telle sorte qu'il puisse exercer efficacement son contrôle. A cet égard, il va de soi que le Comité permanent R, comme il le fait remarquer dans son avis (point 15), doit également avoir la possibilité de consulter les fichiers de journalisations. Cette possibilité ressort d'ailleurs de la compétence générale de contrôle du Comité permanent R, tel qu'organisée par la loi du 18 juillet 1991 y relative, et de sa nouvelle compétence, en tant qu'autorité de protection des données pour les services de renseignement et de sécurité, dont les modalités sont également fixées dans la loi du 18 juillet 1991.

Si la raison du traitement doit également être enregistrée – à distinguer de la finalité légale poursuivie qui demeure de manière générale l'exercice des missions des services de renseignement et de sécurité (point 16 de l'avis du Comité permanent *R)*, il est alors prévu que cette raison et le traitement lui-même soient enregistrés au sein du service de renseignement concerné (et non au sein de la banque de données). Le Comité permanent R relève à ce sujet que le projet n'impose la journalisation du motif de l'accès que si c'est requis par une loi ou en vertu de celle-ci (point 16 de son avis). Il convient de préciser qu'il s'agit, pour l'heure, de l'exécution de l'article 16/4 de la loi du 30 novembre 1998 (accès aux données ANPR). Le Comité permanent R estime cependant que le motif devrait toujours être journalisé, ne serait-ce que de manière sommaire, pour rendre le contrôle ex ante efficace. Comme souligné plus haut, le Comité permanent R dispose d'un accès à tous les traitements et à leurs journalisations dans le cadre de l'exercice de son contrôle, organisé par la loi 18 juillet 1991 susvisée. Il y a lieu de remarquer que les consultations ont toujours un lien avec une enquête dont les éléments sont enregistrés dans la banque de données du service de renseignement concerné, puisqu'elles servent à alimenter ces enquêtes. La raison de la consultation est donc parfaitement retraçable lorsque le Comité permanent R compare les éléments faisant l'objet de la consultation avec les éléments d'enquête enregistrés dans la banque de données du service concerné. De facto, la recommandation du Comité permanent R est rencontrée dans la pratique. Cette précision est également valable pour la journalisation recommandée au point 18 de l'avis du Comité permanent R.

La protection obligatoire de la motivation des traitements se justifie par la nécessité de protéger notamment les sources, les agents ainsi que la discrétion des enquêtes de renseignement. En outre, la raison du traitement est la plupart du temps classifiée au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. Elle ne peut donc être conservée que sur un réseau classifié.

Une dérogation est prévue si cette protection ne se justifie pas. Par exemple, la consultation d'une banque de données dans le cadre d'une vérification de sécurité en application de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, est une procédure officielle, connue de la personne concernée, qui ne justifie pas nécessairement la protection spécifique supplémentaire prévue dans la loi. Pour éviter la confusion qui apparaît dans le point 17 de l'avis du Comité permanent R, le texte a été clarifié, pour préciser que si la journalisation des traitements d'un service de renseignement n'est pas réalisée en son sein, elle le sera dans la banque de données consultée. Dans ce cas, la sauvegarde des consultations est effectuée par le responsable du traitement de la banque de données consultée en cette qualité et en application des prescriptions légales. Ce dernier n'agit dès lors pas pour le compte des services de renseignement et par conséquent n'intervient pas en tant que sous-traitant.

In toepassing van artikel 95 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens wordt het Vast Comité I aangewezen als gegevensbeschermingsautoriteit voor de inlichtingendiensten. De woorden "Commissie voor de bescherming van de persoonlijke levenssfeer" worden dus vervangen, in toepassing van artikel 253 van de eerder vermelde wet van 30 juli 2018, door de woorden "Vast Comité I".

Artikel 6 van dit ontwerp voegt ook nieuwe leden in over de logbestanden van verwerkingen.

Alle verwerkingen in een gegevensbank moeten geregistreerd worden. Omdat de verwerkingen van de inlichtingendiensten niet zichtbaar mogen zijn voor allen die toegang hebben tot de gegevensbank worden er veiligheidsmaatregelen op toegepast.

Het ontwerp voorziet dat deze maatregelen ter beschikking gesteld worden van het Vast Comité I, zodat het zijn controle op een efficiënte wijze kan uitoefenen. In dit opzicht spreekt het vanzelf dat het Vast Comité I, zoals het in zijn advies (punt 15) doet opmerken, ook de logbestanden moet kunnen raadplegen. Deze mogelijkheid vloeit trouwens voort uit de algemene controlebevoegdheid van het Vast Comité I, zoals die wordt georganiseerd bij de betreffende wet van 18 juli 1991, en uit zijn nieuwe bevoegdheid als gegevensbeschermingsautoriteit voor de inlichtingen- en veiligheidsdiensten, waarvan de nadere regels ook in de wet van 18 juli 1991 vastgelegd zijn.

Indien de reden voor de verwerking eveneens geregistreerd moet worden – te onderscheiden van het nagestreefde juridische doeleinde wat over het algemeen de uitoefening van de opdrachten van de inlichtingen- en veiligheidsdiensten blijft (punt 16 van het advies van het Vast Comité *I)*, wordt voorzien dat deze reden en de verwerking zelf dan geregistreerd worden binnen de betrokken inlichtingendienst (en niet binnen de gegevensbank). Het Vast Comité I vestigt hieromtrent de aandacht op het feit dat het ontwerp enkel het loggen van de reden voor de toegang oplegt indien dit door of krachtens een wet wordt vereist (punt 16 van zijn advies). Hierbij moet worden verduidelijkt dat het op dit ogenblik gaat om de uitvoering van artikel 16/4 van de wet van 30 november 1998 (toegang tot ANPR-gegevens). Het Vast Comité I is echter van mening dat de reden altijd moet worden gelogd, al is het maar beknopt, om de controle ex ante efficiënt te maken. Zoals hierboven werd benadrukt, beschikt het Vast Comité I over toegang tot alle verwerkingen en hun logbestanden in het kader van de uitoefening van zijn controle, georganiseerd door de bovenbedoelde wet van 18 juli 1991. Hierbij moet worden opgemerkt dat de raadplegingen altijd verband houden met een onderzoek waarvan de elementen in de gegevensbank van de betrokken inlichtingendienst worden geregistreerd, omdat ze dienen om bij te dragen tot deze onderzoeken. De reden voor de raadpleging kan dus volledig getraceerd worden wanneer het Vast Comité I de elementen van de raadpleging vergelijkt met de onderzoekselementen die in de gegevensbank van de betrokken dienst geregistreerd zijn. Aan de aanbeveling van het Vast Comité I wordt dus de facto in de praktijk tegemoetgekomen. Deze verduidelijking geldt ook voor het loggen dat wordt aanbevolen in punt 18 van het advies van het Vast Comité I.

De verplichte bescherming van de motivering van de verwerkingen wordt gerechtvaardigd door de noodzaak om met name de bronnen, de agenten en de discretie van de inlichtingenonderzoeken te beschermen. Bovendien wordt de reden voor de verwerking meestal geclassificeerd in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen. Zij kan dan ook enkel op een geclassificeerd netwerk worden bewaard.

Een afwijking is voorzien indien deze bescherming niet gerechtvaardigd is. Zo is bijvoorbeeld de raadpleging van een gegevensbank in het kader van een veiligheidsverificatie in toepassing van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen een officiële procedure die gekend is door de betrokkene, wat niet noodzakelijk de specifieke, bijkomende bescherming rechtvaardigt voorzien in de wet. Om de verwarring die blijkt uit punt 17 van het advies van het Vast Comité I te vermijden, werd de tekst verhelderd om te verduidelijken dat indien het loggen van de verwerkingen van een inlichtingendienst niet door de dienst zelf wordt uitgevoerd, dit in de geraadpleegde gegevensbank zal gebeuren. In dit geval wordt de bewaring van de raadplegingen uitgevoerd door de verantwoordelijke voor de verwerking van de geraadpleegde databank in die hoedanigheid en in toepassing van de wettelijke voorschriften. Deze laatste handelt dus niet voor rekening van de inlichtingendiensten en komt bijgevolg niet tussen als verwerker.

Dans son avis (points 15 et 19), le Comité permanent R attire l'attention sur la nécessaire compatibilité entre le présent projet et les articles 13 et 47 de la loi protection des données au sujet du contrôle des logs. A cet égard, il est clair que les mesures de sécurité mises en œuvre pour protéger les traitements des services de renseignement ne peuvent pas empêcher le contrôle légalement prévu sur leur légalité. Les modalités fixées par le présent projet sont parfaitement en conformité avec les articles 13 et 47 précités. En pratique, la mission de contrôle attribuée au responsable du traitement et au délégué à la protection des données (DPO) s'exerce en concertation avec le DPO du service de renseignement concerné.

La première phrase de l'ancien aliéna 2 est supprimée car les alinéas insérés portent sur l'ensemble des données de journalisation.

Afin d'assurer une communication électronique qui permet une exploitation rapide, facile et sous un format compatible, l'exigence de présenter une carte de légitimation est supprimée. En effet, la procédure de demande digitale ne permet pas une telle présentation. Bien entendu, la personne qui demande doit être agent d'un service de renseignement et de sécurité et garantir cette qualité à son interlocuteur. Il va de soi que cet agent n'est autorisé à avoir accès aux informations que dans la mesure où celles-ci sont utiles dans l'exercice de sa fonction, conformément à ce qui est prévu aux articles 13 de la loi du 30 novembre 1998 et 83 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Dans le point 13 de son avis, le Comité permanent R fait remarquer que le dirigeant du service ne pourra désigner sur la liste des personnes ayant un accès à une banque de données externe, que les personnes dont le droit d'accès est justifié « de par leur fonction et sur la base d'un besoin manifeste ». Cette limitation des accès individuels devrait, selon le Comité permanent R, être précisée dans le projet d'arrêté royal. Le gouvernement ne souscrit pas à cette recommandation, dès lors que ce principe est une application générale du principe du besoin d'en connaître consacré par la loi 'protection des données' et par l'article 13, alinéa 4 de la loi du 30 novembre 1998. Il n'y a dès lors pas lieu de l'ajouter dans chaque disposition règlementaire.

Article 7

L'article 4 de l'arrêté royal du 12 octobre 2010 est abrogé car il constitue à présent une redite de l'article 91 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Néanmoins, un nouvel article 13/1 est inséré sous le chapitre VI dont l'intitulé est adapté pour y rassembler toutes les dispositions traitant des données à caractère personnel (voir infra). Ce nouvel article fixe les modalités de désignation du délégué à la protection des données, en exécution de l'article 91 de la loi du 30 juillet 2018. Son application porte sur tous les traitements des services de renseignement, pas uniquement sur ceux qui sont réalisés dans des banques de données externes auxdits services, comme on aurait pu le croire au regard de la situation de l'article 4 dans le chapitre III, quod non.

Article 8

L'article 8 a pour objet d'adapter le chapitre IV.

Tout d'abord, la « Section 1ère. — Des identités et qualités fictives » qui se trouve sous le « Chapitre IV. — Des méthodes spécifiques et des méthodes exceptionnelles de recueil des données » est abrogée puisque les identités et qualités fictives sont dorénavant reprises dans les mesures de protection et d'appui. L'article 6 de l'arrêté royal du 12 octobre 2010 fixant les modalités d'utilisation des identités et qualités fictives est donc supprimé. Les modalités sont maintenant reprises à l'article 2 adapté par le présent projet.

Ensuite, la section 2 « Des modalités de destruction des enregistrements, transcriptions et traductions éventuelles des communications » est renumérotée en section 1ère et les mots « transcriptions et traductions éventuelles des communications » sont supprimés dans son intitulé. Ces mots sont également supprimés à l'article 7 portant exécution de l'article 18/17, § 7 de la loi du 30 novembre 1998. L'article 18/17, § 7 a été adapté par la loi du 30 mars 2017. Cet article qui prévoyait la destruction des enregistrements, transcriptions et traductions éventuelles des communications dans les cinq ans, ne traite plus que de la destruction des enregistrements.

In zijn advies (punten 15 en 19) vestigt het Vast Comité I de aandacht op de vereiste overeenstemming tussen dit ontwerp en de artikelen 13 en 47 van de wet inzake gegevensbescherming met betrekking tot de controle van de logs. In dit opzicht is het duidelijk dat de veiligheidsmaatregelen die aangewend worden om de verwerkingen van de veiligheidsdiensten te beschermen, de wettelijk voorziene controle van hun wettelijkheid niet mogen verhinderen. De in dit ontwerp vastgelegde nadere regels zijn volledig in overeenstemming met de bovengenoemde artikelen 13 en 47. De controleopdracht toegewezen aan de verantwoordelijke voor de verwerking en de functionaris voor gegevensbescherming (DPO) wordt in de praktijk in overleg met de DPO van de betrokken veiligheidsdienst uitgeoefend.

De eerste zin van het vroegere tweede lid wordt geschrapt, aangezien de ingevoegde leden betrekking hebben op het geheel van de logbestandgegevens.

Met het oog op een elektronische communicatie die een snelle, vlotte exploitatie in compatibel formaat mogelijk maakt, wordt de verplichting tot vertoon van een legitimatiekaart geschrapt. De digitale aanvraagprocedure laat een vertoon in die zin immers niet toe. De persoon achter de aanvraag moet uiteraard een agent van een inlichtingen- en veiligheidsdienst zijn, en die hoedanigheid garanderen ten aanzien van zijn gesprekspartner. Die agent is uiteraard enkel gemachtigd om toegang te krijgen tot de informatie voor zover deze nuttig is voor de uitoefening van zijn functie, zulks overeenkomstig het bepaalde in de artikelen 13 van de wet van 30 november 1998 en 83 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

In punt 13 van zijn advies doet het Vast Comité I opmerken dat het diensthoofd op de lijst van personen die toegang hebben tot een externe gegevensbank enkel de personen kan aanwijzen voor wie het toegangsrecht gerechtvaardigd is "als gevolg van hun ambt en op basis van een duidelijke behoefte". Deze beperking van de individuele toegangen zou volgens het Vast Comité I in het ontwerp van koninklijk besluit verduidelijkt moeten worden. De regering is het niet eens met deze aanbeveling, aangezien dit beginsel een algemene toepassing is van het beginsel van de noodzaak tot kennisname verankerd in de wet inzake gegevensbescherming en in artikel 13, vierde lid van de wet van 30 november 1998. Het dient dus niet in elke reglementaire bepaling toegevoegd te worden.

Artikel 7

Artikel 4 van het koninklijk besluit van 12 oktober 2010 wordt afgeschaft gezien het een herhaling is van artikel 91 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

In plaats hiervan wordt een nieuw artikel 13/1 ingevoegd onder het hoofdstuk VI waarvan het opschrift wordt aangepast om er alle bepalingen inzake de verwerking van persoonsgegevens te verzamelen (zie infra). Dit nieuwe artikel legt de nadere regels vast voor de aanwijzing van een functionaris voor gegevensbescherming in toepassing van artikel 91 van de wet van 30 juli 2018. Het is van toepassing op alle verwerkingen van de inlichtingendiensten, niet enkel op diegene die uitgevoerd worden in gegevensbanken die extern zijn aan de diensten, wat men had kunnen afleiden uit de plaatsing van artikel 4 in het hoofdstuk III, quod non.

Artikel 8

Artikel 8 heeft tot doel hoofdstuk IV aan te passen.

Allereerst wordt "Afdeling 1 – Fictieve identiteiten en hoedanigheden" die zich in "Hoofdstuk IV – Specifieke methoden en uitzonderlijke methoden voor het verzamelen van gegevens" bevindt, opgeheven omdat de fictieve identiteiten en hoedanigheden voortaan in de beschermings- en ondersteuningsmaatregelen opgenomen zijn. Artikel 6 van het koninklijk besluit van 12 oktober 2010 dat de nadere regels voor het gebruik van fictieve identiteiten en hoedanigheden vastlegt, wordt dus geschrapt. De nadere regels zijn nu in het door dit ontwerp aangepaste artikel 2 opgenomen.

Vervolgens wordt afdeling 2 "Nadere regels voor de vernietiging van de opnamen en van de eventuele overschrijvingen en vertalingen van de communicaties" vernummerd tot afdeling 1 en de woorden "de eventuele overschrijvingen en vertalingen van de communicaties" worden in het opschrift geschrapt. Deze woorden worden ook geschrapt in artikel 7 houdende uitvoering van artikel 18/17, § 7 van de wet van 30 november 1998. Artikel 18/17, § 7 werd door de wet van 30 maart 2017 aangepast. Dit artikel dat de vernietiging van de opnamen en van de eventuele overschrijvingen en vertalingen van de communicaties binnen de vijf jaar voorzag, behandelt enkel nog de vernietiging van de opnamen.

L'intitulé de la section 2 du chapitre IV et l'article 7 de l'arrêté royal du 12 octobre 2010 sont donc adaptés pour ne plus mentionner les transcriptions et traductions éventuelles des communications.

Enfin, l'article 8 renumérote la section 3 « De la rétribution de la collaboration des personnes physiques et des personnes morales » en section 2.

Article 9

L'article 18/10 § 4 ayant été adapté par la loi du 30 mars 2017, l'article 10 de l'arrêté royal du 12 octobre 2010, qui exécute cet article, doit être adapté en ce sens.

Article 10

L'obligation de tenir des listes mensuelles des mesures spécifiques ayant été mises en œuvre a été supprimée à l'article 18/3, § 2 de la loi du 30 novembre 1998, par la loi du 30 mars 2017.

Dès lors, l'alinéa 1er de l'article 43/3 de la loi du 30 novembre 1998 qui déterminait les modalités de notification de ces listes a également été abrogé par la loi du 30 mars 2017, ce qui entraîne, à son tour, l'inanité de son exécution. L'alinéa 1er de l'article 11 de l'arrêté royal du 12 octobre 2010 qui exécutait l'article 43/3, alinéa 1er est donc supprimé.

L'alinéa 2 de l'article 43/3 a été simplifié et complété pour faire référence à tous les types d'« actes » pouvant être pris. L'alinéa 2 de l'article 11 est reformulé dans le même sens.

En réponse au point 22 de l'avis du Comité permanent R, il a été ajouté dans le projet que la commission doit lui communiquer le moment où la décision lui a été notifiée. Par contre, il n'est pas nécessaire d'ajouter la communication d'une prolongation car celle-ci est toujours mentionnée dans la décision ou l'autorisation elle-même et le Comité R permanent recevant toutes les décisions, autorisations et avis, il est déjà en possession de cette information.

Le quatrième alinéa de l'article 11 de l'arrêté royal du 12 octobre 2010 imposait que certaines données soient mentionnées dans les décisions, avis et autorisations. Ces mentions ayant été reprises aux articles 18/3 et 18/10 de la loi du 30 novembre 1998, cet alinéa n'a plus d'utilité. Il est abrogé.

Article 11

En application de l'article 91 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, « le conseiller en sécurité de l'information et en protection de la vie privée » s'appelle désormais le « délégué à la protection des données ».

L'article 12 de l'arrêté royal du 12 octobre 2010 est adapté en ce sens.

Article 12

L'intitulé du chapitre VI est adapté pour y rassembler toutes les dispositions traitant des données à caractère personnel.

Article 13

Le présent article insère un nouvel article 13/1 en exécution de l'article 91 de la loi du 30 juillet 2018.

La règle selon laquelle un délégué à la protection des données doit être désigné au sein de chaque service de renseignement était déjà consacrée à l'article 4 de l'arrêté royal du 12 octobre 2010. A présent, la règle a été transcrite dans la loi du 30 juillet 2018, rendant l'article 4 obsolète.

La nouvelle disposition introduite dans l'arrêté royal détermine les modalités de désignation et les conditions exigées pour exercer la fonction de délégué à la protection des données. En raison du caractère secret du travail des services de renseignement et de l'aspect délicat de leurs banques de données, seul un membre du service concerné pourra être désigné pour exercer cette fonction.

A l'instar de ce que prévoyait l'article 4 de l'arrêté royal, le paragraphe 2 précise que le délégué à la protection des données peut également remplir la fonction de conseiller à la sécurité des données, telle qu'elle est prévue dans différentes réglementations, notamment à l'article 6 de l'arrêté royal du 28 février 2002 relatif à la transmission d'informations par les communes, à la Sûreté de l'Etat, par l'intermédiaire du registre national des personnes physiques et à l'article 20 de la loi du 15 août 2012 relative à la création et à l'organisation de l'intégrateur de services fédéral. » La terminologie 'conseiller à la

Het opschrift van afdeling 2 van hoofdstuk IV en artikel 7 van het koninklijk besluit van 12 oktober 2010 worden dus zodanig aangepast dat ze de eventuele overschrijvingen en vertalingen van de communicaties niet meer vermelden.

Ten slotte vernummert artikel 8 afdeling 3 "De vergoeding voor de medewerking van natuurlijke personen en rechtspersonen" tot afdeling 2.

Artikel 9

Aangezien artikel 18/10 § 4 door de wet van 30 maart 2017 werd aangepast, moet artikel 10 van het koninklijk besluit van 12 oktober 2010, dat dit artikel uitvoert, in die zin worden aangepast.

Artikel 10

De verplichting om maandelijkse lijsten van de aangewende specifieke methoden bij te houden, werd door de wet van 30 maart 2017 geschrapt in artikel 18/3, § 2 van de wet van 30 november 1998.

Bijgevolg werd het 1ste lid van artikel 43/3 van de wet van 30 november 1998 dat de nadere regels voor de kennisgeving van deze lijsten bepaalde, ook opgeheven door de wet van 30 maart 2017 wat op zijn beurt de zinloosheid van de uitvoering ervan met zich meebrengt. Het 1ste lid van artikel 11 van het koninklijk besluit van 12 oktober 2010 dat artikel 43/3, 1ste lid uitvoerde, wordt dus geschrapt.

Lid 2 van artikel 43/3 werd vereenvoudigd en aangevuld om te verwijzen naar alle types "handelingen" die genomen kunnen worden. Leden 2 en 3 van artikel 11 werden in dezelfde zin geherformuleerd.

In antwoord op punt 22 van het advies van het Vast Comité I werd in het ontwerp toegevoegd dat de commissie het Comité moet meedelen wanneer de beslissing haar ter kennis werd gebracht. Daarentegen is het niet nodig om de mededeling van een verlenging toe te voegen, omdat die altijd vermeld wordt in de beslissing of de machtiging zelf en aangezien het Vast Comité I alle beslissingen, machtigingen en adviezen ontvangt, is het reeds in het bezit van deze informatie.

Het vierde lid van artikel 11 van het koninklijk besluit van 12 oktober 2010 legde op dat bepaalde gegevens in de beslissingen, adviezen en machtigingen vermeld werden. Aangezien deze vermeldingen in artikelen 18/3 en 18/10 van de wet van 30 november 1998 opgenomen werden, heeft dit lid geen nut meer. Het wordt opgeheven.

Artikel 11

In toepassing van artikel 91 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, heet "de raadgever informatieveiligheid en bescherming van de persoonlijke levenssfeer" voortaan "de functionaris voor gegevensbescherming".

Artikel 12 van het koninklijk besluit van 12 oktober 2010 wordt aangepast in die zin.

Artikel 12

Het opschrift van hoofdstuk VI wordt aangepast om er alle bepalingen over de verwerking van persoonsgegevens in onder te brengen.

Artikel 13

Dit artikel voegt een nieuw artikel 13/1 in ter uitvoering van artikel 91 van de wet van 30 juli 2018.

De regel volgens dewelke een functionaris voor gegevensbescherming moet worden aangewezen binnen elke inlichtingendienst werd reeds vastgelegd in artikel 4 van het koninklijk besluit van 12 oktober 2010. Momenteel is de regel opgenomen in de wet van 30 juli 2018, wat artikel 4 overbodig maakt.

De nieuwe bepaling die ingevoegd werd in het koninklijk besluit bepaalt de nadere aanwijzingsregels en de vereiste voorwaarden om de functie van functionaris voor gegevensbescherming uit te oefenen. Wegens het geheime karakter van het werk van de inlichtingendiensten en het gevoelige karakter van hun gegevensbanken kan enkel een lid van de betrokken inlichtingendienst aangewezen worden om deze functie uit te oefenen.

Naar analogie van het bepaalde in artikel 4 van het koninklijk besluit wordt in paragraaf 2 verduidelijkt dat de functionaris voor gegevensbescherming ook de functie van raadsman voor de veiligheid van de gegevens kan vervullen, zoals bepaald in verschillende regelgevingen, inzonderheid in artikel 6 van het koninklijk besluit van 28 februari 2002 betreffende de mededeling van informatie door de gemeenten aan de Veiligheid van de Staat door toedoen van het Rijksregister van de natuurlijke personen en in artikel 20 van de wet van 15 augustus 2012 houdende oprichting en organisatie van een

sécurité des données' couvre celle de conseiller en sécurité de l'information et autres terminologies qui renvoient à la fonction consistant à veiller au respect de la loi lors de toute demande de données et à prendre toutes mesures utiles afin d'assurer la sécurité des informations enregistrées.

Article 14

Le présent article adapte l'article 14 de l'arrêté royal du 12 octobre 2010 pour le rendre conforme à la nouvelle règlementation sur le traitement des données à caractère personnel.

Article 15

Un nouveau chapitre III/1 a été inséré dans la loi du 30 novembre 1998 par la loi du 30 mars 2017. Il traite de la protection du personnel, des infrastructures et des biens des services de renseignement.

L'article 27 de ce chapitre doit être exécuté, raison pour laquelle un nouveau chapitre VII est inséré dans l'arrêté royal du 12 octobre 2010.

Article 16

Un nouvel article 15 est inséré pour fixer les modalités d'enregistrement de l'arrestation visée à l'article 27 de la loi du 30 novembre 1998 ainsi que les modalités de conservation des données en lien avec cette arrestation.

Ce nouvel article 15 dispose qu'un registre doit être tenu par le dirigeant du service ou la personne qu'il désigne à cet effet. Il contient la date, le contexte et les éventuels incidents survenus. Ces données doivent être conservées minimum cinq ans à dater de l'arrestation.

Pour répondre au point 4 de l'avis du Comité permanent R, le délai de conservation a été porté à dix ans, comme pour les logs dans les banques de données et pour les journaux de bord des identités fictives (actuel article 6). En s'alignant sur ce délai, on obtient en effet l'harmonisation des délais de conservation.

Article 17

Le Chapitre VII est renuméroté Chapitre VIII.

Article 18

Les articles 15 et 16 sont renumérotés respectivement articles 16 et 17.

Dans son avis, le Conseil d'Etat déconseille de renuméroter des articles, principalement pour éviter des problèmes de référence dans d'autres textes. Cet avis n'a pas été suivi car en réalité, il s'agit de renumérotation de sections, d'un chapitre et de deux articles contenant des dispositions finales. Ces dispositions n'ayant pas fait l'objet de référence dans d'autres textes, le problème ne se pose pas.

CHAPITRE II. — *Modification de l'arrêté royal du 3 juillet 2016 portant exécution de l'article 21 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité*

Articles 19 et 20

La loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel abroge 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 impose la désignation d'un délégué à la protection des données.

En exécution de l'article 253, alinéa 2 de la loi 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, les présents articles modifient les références faites à la loi et au conseiller en sécurité de l'information dans les articles 1er et 4 de l'arrêté royal du 3 juillet 2016.

Le Ministre de la Justice,
K. GEENS

Le Ministre de la Défense,
D. REYNDERS

federale dienstenintegrator. De terminologie "raadsman voor de veiligheid van de gegevens" omvat die van raadgever informatieveiligheid en andere terminologieën die verwijzen naar de functie die erin bestaat toe te zien op de inachtneming van de wet bij enig verzoek om gegevens en alle nuttige maatregelen te nemen om de veiligheid van de geregistreerde informatie te waarborgen.

Artikel 14

Dit artikel wijzigt artikel 18 van het koninklijk besluit van 12 oktober 2010 om het in overeenstemming te brengen met de nieuwe regelgeving inzake de verwerking van persoonsgegevens.

Artikel 15

Een nieuw hoofdstuk III/1 werd door de wet van 30 maart 2017 in de wet van 30 november 1998 ingevoegd. Het behandelt de bescherming van het personeel, de infrastructuur en de goederen van de inlichtingendiensten.

Artikel 27 van dit hoofdstuk moet worden uitgevoerd. Om die reden wordt in het koninklijk besluit van 12 oktober 2010 een nieuw hoofdstuk VII ingevoegd.

Artikel 16

Een nieuw artikel 15 wordt ingevoegd om de nadere regels voor het registreren van de aanhouding bedoeld in artikel 27 van de wet van 30 november 1998 vast te leggen alsook de nadere regels voor het bewaren van gegevens over deze aanhouding.

Dit nieuwe artikel 15 bepaalt dat er een register moet worden bijgehouden door het diensthoofd of de persoon die hij hiertoe aanstelt. Het bevat de datum, de context en eventuele incidenten die zich hebben voorgedaan. Deze gegevens moeten minstens vijf jaar vanaf de datum van de aanhouding bewaard worden.

Om te beantwoorden aan punt 4 van het advies van het Vast Comité I werd de bewaartermijn op tien jaar gebracht, zoals voor de logs van de gegevensbanken en voor de logboeken van de fictieve identiteiten (huidig artikel 6). Door zich op deze termijn af te stemmen verkrijgt men inderdaad de harmonisering van bewaartermijnen.

Artikel 17

Hoofdstuk VII wordt tot hoofdstuk VIII vernummerd.

Artikel 18

Artikelen 15 en 16 worden tot respectievelijk artikelen 16 en 17 vernummerd.

In zijn advies raadt de Raad van State af om artikelen te vernummeren, voornamelijk om problemen met verwijzingen in andere teksten te vermijden. Dit advies werd niet gevolgd, omdat het in werkelijkheid gaat om de vernummering van afdelingen, van een hoofdstuk en van twee artikelen die de slotbepalingen bevatten. Aangezien naar deze bepalingen niet wordt verwezen in andere teksten, stelt het probleem zich niet.

HOOFDSTUK II. — *Wijziging van het koninklijk besluit van 3 juli 2016 houdende uitvoering van artikel 21 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten*

Artikelen 19 en 20

De wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens schaft de wet van 8 december 1992 tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens af en legt de aanwijzing van een functionaris voor gegevensbescherming op.

Ter uitvoering van artikel 253, lid 2 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, wijzigen deze artikelen de verwijzingen naar de wet en naar de raadgever informatieveiligheid en bescherming van de persoonlijke levenssfeer in de artikelen 1 en 4 van het koninklijk besluit van 3 juli 2016.

De Minister van Justitie,
K. GEENS

De Minister van Defensie,
D. REYNDERS

COMITE PERMANENT DE CONTROLE DES SERVICES DE RENSEIGNEMENTS ET DE SECURITE. — AVIS 002/CPR-ACC/2019 DU 9 AVRIL 2019. — Modification de l'A.R. du 12 octobre 2010 et de l'A.R. du 3 juillet 2016

PROJET D'ARRÊTÉ ROYAL MODIFIANT L'ARRÊTÉ ROYAL DU 12 OCTOBRE 2010 PORTANT EXÉCUTION DE DIVERSES DISPOSITIONS DE LA LOI DU 30 NOVEMBRE 1998 ORGANIQUE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ ET DE L'ARRÊTÉ ROYAL DU 3 JUILLET 2016 PORTANT EXÉCUTION DE L'ARTICLE 21 DE LA LOI DU 30 NOVEMBRE 1998 ORGANIQUE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ

1. Dans son courriel du 8 mars 2019, le ministre de la Justice a demandé au Comité permanent R de rendre un avis sur l' 'Avant-projet de modification de l'Arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et de l'Arrêté royal du 3 juillet 2016 portant exécution de l'article 21 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité'.

Dans la demande, il n'est pas précisé sur la base de quelle disposition légale l'avis est sollicité. Le Comité a décidé de rendre un avis en sa qualité d'organe de contrôle des services de renseignement (art. 33, alinéa 8 Loi Contrôle du 18 juillet 1991) *et*en sa qualité d'autorité de contrôle sur les traitements des données à caractère personnel par les services de renseignement (art. 95 de la Loi protection des données du 30 juillet 2018). Cette seconde qualité est requise puisque le projet d'arrêté veut donner exécution à l'article 16/4 de la Loi du 30 novembre 1998, et qu'à cet effet, le Roi doit demander l'avis préalable de 'l'autorité de protection des données compétente', en l'occurrence le Comité permanent R.

2. Le projet d'arrêté proposé donne exécution à trois lois :

- la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD), qui a désigné le Comité permanent R comme autorité de protection des données pour le traitement des données à caractère personnel par les services de renseignement et qui a introduit quelques autres dispositions. Celles-ci impliquent des adaptations, d'une part de l'Arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité et, d'autre part, de l'Arrêté royal du 3 juillet 2016 portant exécution de l'article 21 de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité' ;

- la Loi du 30 mars 2017 qui apporte de nombreuses modifications à la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S) ;

- la Loi du 21 mars 2018 modifiant la Loi sur la fonction de police en vue de régler l'utilisation de caméras par les services de police, et modifiant la Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la Loi du 2 octobre 2017 réglementant la sécurité privée et particulière qui a inséré l'article 16/4 dans la L.R&S, permettant aux services de renseignement d'avoir accès aux informations et données à caractère personnel qui sont collectées au moyen de caméras utilisées par les services de police.

3. Le Comité permanent R limite ses commentaires à plusieurs modifications proposées à l'Arrêté royal du 21 octobre 2010. Le Comité souscrit à toutes les autres dispositions modificatives.

Le délai de conservation pour les journaux de bord et le registre des arrestations

4. Les propositions d'articles 2, 2/1 et l'A.R. du 12 octobre 2010 prévoient que les journaux de bord et le registre des arrestations requis soient conservés respectivement *'au minimum pendant cinq ans après la dernière utilisation du faux nom, de l'identité ou de la qualité fictive'*, *'au minimum pendant cinq ans après la dissolution ou la liquidation de que la personne morale'* ou *'pendant minimum cinq ans après l'arrestation'*.

Le Comité ne voit pas pourquoi ces données

– qui nécessitent d'ailleurs peu de capacités de stockage – devraient déjà être théoriquement détruites après cinq ans. Une telle destruction rend impossible tout contrôle ultérieur par le Comité, qui fait remarquer que l'A.R. du 12 octobre 2010 prévoit déjà un délai de conservation de dix ans pour les logs dans les banques de données du secteur public (art. 3 § 1er) ou pour les journaux de bord reprenant l'identité ou la

VAST COMITE VAN TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN. — ADVIES 002/VCI-BTA/2019 VAN 9 APRIL 2019. — Wijziging KB 12 oktober 2010 en KB 3 juli 2016

VOORONTWERP VAN KONINKLIJK BESLUIT TOT WIJZIGING VAN HET KONINKLIJK BESLUIT VAN 12 OKTOBER 2010 HOUDENDE UITVOERING VAN DIVERSE BEPALINGEN VAN DE WET VAN 30 NOVEMBER 1998 HOUDENDE REGELING VAN DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN EN HET KONINKLIJK BESLUIT VAN 3 JULI 2016 HOUDENDE UITVOERING VAN ARTIKEL 21 VAN DE WET VAN 30 NOVEMBER 1998 HOUDENDE REGELING VAN DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

1. Bij mailbericht van 8 maart 2019 vroeg de minister van Justitie aan het Vast Comité I zijn advies te verlenen bij het 'Voorontwerp van wijziging van het Koninklijk besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en het Koninklijk besluit van 3 juli 2016 houdende uitvoering van artikel 21 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheids-diensten'.

Het verzoek specifieert niet nader op basis van welke wettelijke bepaling het advies wordt verzocht. Het Comité besloot om het advies te verlenen zowel in zijn hoedanigheid van toezichthouder op de inlichtingendiensten (art. 33, achtste lid Toezichtwet van 18 juli 1991) als in zijn hoedanigheid van toezichthoudende autoriteit op de verwerkingen van persoonsgegevens door de inlichtingendiensten (art. 95 Gegevensbeschermingswet van 30 juli 2018). Dit laatste is vereist aangezien het ontwerpbesluit uitvoering wil geven aan artikel 16/4 van de Wet van 30 november 1998 en de Koning hiertoe het voorafgaand advies van 'de bevoegde toezichthoudende autoriteit voor de verwerking van persoonsgegevens' – *in casu* het Vast Comité I – moet inwinnen.

2. Het voorgestelde ontwerpbesluit geeft uitvoering aan drie wetten:

- de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (GBW) die het Vast Comité I als gegevensbeschermingsautoriteit voor de verwerking van persoonsgegevens door de inlichtingendiensten heeft aangewezen en waarbij enkele andere bepalingen werden ingevoerd die aanpassingen vereisen aan enerzijds het Koninklijk besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en anderzijds het Koninklijk besluit van 3 juli 2016 houdende uitvoering van artikel 21 van de Wet van 30 november 1998;

- de Wet van 30 maart 2017 die talrijke wijzigingen aanbracht aan de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (W.I&V);

- 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 waarbij artikel 16/4 in de W.I&V werd ingevoegd om inlichtingendiensten toe te laten toegang te hebben tot informatie en persoonsgegevens die verzameld worden door middel van door de politiediensten gebruikte camera's.

3. Het Vast Comité I formuleert alleen bemerkingen bij een aantal wijzigingen die worden voorgesteld aan het Koninklijk besluit van 12 oktober 2010. Het Comité kan zich vinden in alle andere wijzigingsbepalingen.

Bewaringstermijn voor de logboeken en het arrestatieregister

4. De voorgestelde artikelen 2, 2/1 en KB 12 oktober 2010 voorzien dat de vereiste logboeken en het arrestatieregister moeten worden bewaard respectievelijk *'gedurende minstens vijf jaar na het laatste gebruik van de valse naam, van de fictieve identiteit of van de fictieve hoedanigheid'*, *'gedurende minstens vijf jaar na de ontbinding of vereffening van de rechtspersoon'* of *'gedurende minstens vijf jaar na de aanhouding'*.

Het Comité ziet niet in waarom deze gegevens

– die overigens nauwelijks opslagcapaciteit vereisen – in theorie reeds na vijf jaar zouden kunnen vernietigd worden. Dergelijke vernietiging maakt elke latere controle door het Comité onmogelijk. Het Comité wijst er op dat het KB van 12 oktober 2010 reeds voorziet in een bewaartermijn van tien jaar voor de logs in de gegevensbanken van de openbare sector (art. 3 § 1) of voor de logboeken waarin de

qualité fictive d'agents qui opèrent au sein de personnes morales fictives (art. 6). Enfin, le Comité attire l'attention sur le fait que l'utilisation d'un faux nom ou d'une fausse qualité, ou encore l'arrestation d'une personne en dehors du cadre légal, peut constituer une infraction, et que le journal de bord/registre à cet égard pourrait être utilisé comme un élément de preuve tant à charge qu'à décharge. Dans cette perspective aussi, une destruction après cinq ans pourrait donner lieu à des complications inutiles. Enfin, il est possible que ces logs se révèlent être pertinents dans d'autres enquêtes pénales auxquelles les services de renseignement ont, par exemple, prêté leur assistance technique ou pour lesquelles ils ont fourni des informations.

Le Comité recommande dès lors d'harmoniser la conservation de ces éléments avec le délai de prescription en matière pénale.

La création de personnes morales en appui du fonctionnement des services de renseignement

5. L'article 13/3 L.R&S dispose que les services de renseignement peuvent créer des personnes morales '*selon les modalités fixées par le Roi. Ces modalités peuvent déroger aux dispositions légales applicables en cas de dissolution et de liquidation d'une personne morale*'. Mais le projet d'arrêté ne définit pas de '*modalités*' pour la création, la dissolution ou la liquidation. L'article 4 du projet d'arrêté établit ce qui suit : 4 : '*Pour répondre à des besoins opérationnels ou de discrétion, le dirigeant du service concerné peut, par décision écrite motivée déroger aux dispositions légales applicables en cas de dissolution ou de liquidation d'une personne morale*'. La mission confiée au Roi par le législateur est ainsi déléguée au dirigeant du service, ce qui n'est pas légalement autorisé.

Accès aux banques de données des secteurs public et privé

6. En ce qui concerne la proposition de réglementation relative à l'accès aux banques de données des secteurs public et privé dans lesquelles sont traitées des données à caractère personnel, le Comité reprend les trois passages importants suivants issus du Rapport au Roi :

- ' *La présente modification de l'arrêté royal n'octroie pas d'accès à une banque de données externe, il détermine seulement les modalités à appliquer lorsqu'un tel accès existe par ou en vertu d'une loi, ou avec le consentement du responsable du traitement de la banque de données.*' ;

- '*L'article 6 adapte l'article 3 de l'arrêté royal du 12 octobre 2010 afin de fixer les modalités d'accès à toute banque de données auxquelles les services de renseignement ont ou auront accès, par ou en vertu d'une loi spécifique ou, sur base des articles 14 (données du secteur public) et 16 (données du secteur privé) de la loi organique, avec le consentement du responsable du traitement de la banque de données*'.

- '*Cet article exécute notamment les articles 14, 16/2 et 16/4 de la loi du 30 novembre 1998*'.

Le Comité permanent R note dès lors que les règles fixées dans le projet d'arrêté valent pour les banques de données de personnes (morales) publiques et privées, et ce tant pour les banques de données auxquelles un service de renseignement a déjà accès (par ou en vertu d'une loi ou avec l'accord des responsables du traitement) que pour banques de données auxquelles il aura accès dans le futur.

7. En ce qui concerne l'accès octroyé par ou en vertu de la loi aux banques de données des autorités publiques, il peut être notamment fait mention de l'accès à des banques de données communes dans lesquelles figurent des données de *terrorist fighters* ou de prédicateurs de haine (voir art. 44/11/3*ter* Loi sur la Fonction de police) ou au Casier judiciaire central (art. 593 CP). La Loi du 30 novembre 1998 autorise les services de renseignement à accéder à certaines banques de données des autorités publiques : le Registre national et les registres de la population (art. 17 L.R&S) et les images de caméras des banques de données visées à l'article 44/2 de la Loi sur la fonction de police et les informations et données à caractère personnel des banques de données visées aux articles 25/6, 44/2, § 3, alinéa 2, 1° et 2°, et 46/12 de la même loi (art. 16/4 L.R&S).

8. En ce qui concerne l'accès octroyé par ou en vertu de la loi aux fichiers qui sont conservés par des personnes (morales) privées, citons, par exemple, l'article 16/2 L.R&S qui dispose que l'on peut procéder à l'identification de personnes qui utilisent un moyen de communication déterminé non seulement par le biais d'une réquisition à l'opérateur ou au fournisseur de services, mais aussi 'au moyen d'un accès aux fichiers des clients', 'dans le respect des principes de proportionnalité et de subsidiarité, et moyennant l'enregistrement de la consultation', et ce dans les 'conditions techniques' fixées par le Roi.

9. Enfin, la possibilité – pas l'obligation – existe pour le responsable du traitement de donner (un) accès (limité ou général) à sa banque de données.

fictieve identiteit of hoedanigheid is opgenomen van agenten die opereren binnen fictieve rechtspersonen (art. 6). Het Comité wijst er ten slotte op dat het hanteren van een valse naam of hoedanigheid of de arrestatie van een persoon buiten het wettelijk kader een misdrijf kan uitmaken en dat het logboek/register in dat verband zou kunnen gehanteerd worden als bewijselement en dit zowel *à charge* als *à décharge*. Ook vanuit dit perspectief zou een vernietiging na vijf jaar voor onnodige moeilijkheden kunnen zorgen. Ten slotte is het mogelijk dat deze logs relevant blijken in andere strafonderzoeken waaraan de inlichtingen-diensten bijvoorbeeld hun technische bijstand hebben verleend of waarbij zij informatie hebben verschaft.

Het Comité beveelt dan ook aan om de bewaring van deze elementen af te stemmen op de verjaringstermijn in strafzaken.

Het oprichten van rechtspersonen ter ondersteuning van de werking van de inlichtingendiensten

5. Artikel 13/3 W.I&V stelt dat de inlichtingendiensten rechtspersonen kunnen oprichten '*volgens de door de Koning te bepalen nadere regels. Die nadere regels kunnen afwijken van de wettelijke bepalingen die van toepassing zijn in geval van ontbinding en vereffening van een rechtspersoon.*' Het ontwerp KB bepaalt echter geen '*nadere regels*' voor de oprichting, de ontbinding of de vereffening. Het ontwerpbesluit stelt het volgende in zijn artikel 4: '*Om te voldoen aan operationele behoeften of behoeften ingegeven door geheimhouding kan het betrokken diensthoofd, bij gemotiveerde schriftelijke beslissing, afwijken van de wettelijke bepalingen die van toepassing zijn in geval van ontbinding of vereffening van een rechtspersoon*'. Op die wijze wordt de door de wetgever aan de Koning toevertrouwde opdracht gedelegeerd naar het diensthoofd, hetgeen wettelijk niet toegelaten is.

Toegang tot gegevensbanken van de openbare en private sector

6. Wat betreft de voorgestelde regeling inzake toegang tot gegevensbanken van de openbare en publieke sector waarin persoonsgegevens verwerkt zijn, herneemt het Comité volgende drie belangrijke passages uit het Verslag aan de Koning:

- '*Deze wijziging van het koninklijk besluit verleent geen toegang tot een externe gegevensbank, het bepaalt enkel de nadere regels die moeten worden toegepast wanneer een dergelijke toegang bestaat door of krachtens een wet of met de toestemming van de verwerkingsverantwoordelijke van de gegevensbank.*';

- '*Artikel 6 wijzigt artikel 3 van het koninklijk besluit van 12 oktober 2010 om de toegangsbepalingen vast te leggen voor elke gegevensbank waartoe de inlichtingen- en veiligheidsdiensten toegang hebben of zullen hebben, door of krachtens een specifieke wet, of, op basis van artikelen 14 (gegevens van het openbare sector) of 16 (gegevens van het private sector), met de toestemming van de verwerkingsverantwoordelijke van de gegevens-bank.*'

- '*Dit artikel voert meer bepaald de artikelen 14, 16/2 en 16/4 van de wet van 30 november 1998 uit.*'

Het Vast Comité I noteert dan ook dat de in het ontwerpbesluit vastgestelde regels dus gelden voor databanken van publieke én private (rechts)personen en dit zowel voor databanken waartoe een inlichtingendienst reeds toegang heeft (door of krachtens een wet of met toestemming van de verwerkings-verantwoordelijke) of in de toekomst toegang zal krijgen.

7. Wat betreft de toegang verleend door of krachtens de wet aan databanken van publieke overheden kan bijvoorbeeld verwezen worden naar de toegang tot de gemeenschappelijke databanken waarin gegevens van *terrorist fighters* of haatpredikers zijn opgenomen (zie art. 44/11/3*ter* Wet op het Politieambt) of het Centraal Strafregister (art. 593 Sv.). Ook de Wet van 30 november 1998 verleent de inlichtingendiensten toegang tot bepaalde databanken van openbare overheden: het Rijksregister en de bevolkingsregisters (art. 17 W.I&V) en camerabeelden uit de gegevensbanken bedoeld in artikel 44/2 Wet op het Politieambt en de informatie en persoonsgegevens van de gegevensbanken bedoeld in artikels 25/6, 44/2, § 3, tweede lid, 1° en 2°, en 46/12 van diezelfde wet (art. 16/4 W.I&V).

8. Wat betreft de toegang verleend door of krachtens de wet aan databestanden die bijgehouden worden door private (rechts)personen kan bijvoorbeeld verwezen worden naar artikel 16/2 W.I&V dat bepaalt dat de identificatie van personen die een bepaald communicatiemiddel gebruiken niet alleen kan via een vordering van de operator of van de dienstenverstrekker maar ook '*met behulp van toegang tot de klantenbestanden*', '*mits naleving van de principes van proportionaliteit en subsidiariteit en mits de registratie van de raadpleging*' en dit onder de door de Koning bepaalde '*technische voorwaarden*'.

9. Ten slotte is er de mogelijkheid – niet de verplichting – voor de verwerkings-verantwoordelijke om (een beperkte of algemene) toegang te verlenen tot zijn databank.

Si ce responsable du traitement est une personne (morale) privée, il n'y a d'obstacles, en principe, que pour les avocats, les médecins et les journalistes. Ils doivent respecter le secret professionnel auquel ils sont tenus ainsi que le secret de leurs sources. Avant la modification de loi de 2017, qui a modifié l'article 16 L.R&S, les particuliers devaient également tenir compte du principe de finalité : les données à caractère personnel qui étaient traitées dans le but A ne pouvaient être transmises sans autre forme de procès à, par exemple, des services de renseignement qui utiliseraient ces données dans un but B. Il en était ainsi parce que l'article 16 L.R&S faisait au départ explicitement référence aux règles en matière de protection des données. En 2017, les termes suivants ont été supprimés: 'Conformément à l'article 3, § 4, de la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel'.

Il n'est cependant pas exclu que des lois spécifiques (existantes ou nouvelles) interdisent encore la transmission à des tiers de (certaines) données à caractère personnel issues de certains fichiers, ou leur en octroient l'accès. Il est donc important qu'avant l'octroi d'un accès, tant les acteurs privés que les services de renseignement vérifient si une obligation de confidentialité spécifique légale est d'application.

Le Comité permanent R souligne à nouveau que la possibilité d'obtenir un accès direct à des banques de données ne peut être utilisée pour contourner des procédures légales qui prévoient un contrôle spécifique. On entend par là, par exemple, l'accès direct à des données de localisation conservées par des entreprises de télécommunication ou des données financières traitées par des institutions bancaires, alors qu'il s'agit d'une méthode spécifique ou exceptionnelle. Dans ces cas-là, aucun accès ni interrogation direct(e) ne peut être organisé(e).

10. Si par ou en vertu de la loi ou après accord avec le responsable du traitement, un accès direct est rendu possible, une série de règles devront au moins être respectées (dans la loi, l'arrêté pris en vertu de la loi ou l'accord, des règles supplémentaires peuvent être formulées). Ces règles figuraient dans le projet d'arrêté. Il convient toutefois de souligner que le projet d'arrêté règle non seulement les modalités d'un 'accès direct', mais aussi d'une '*interrogation directe*'. Mais le projet ne précise pas ce qu'il y a lieu d'entendre par là. Le Comité recommande que l'A.R. définisse plus avant ces termes. En outre, il est préférable de s'inscrire dans la définition reprise à l'article 44/11/4 de la Loi sur la fonction de police. '*Par 'accès direct', il faut entendre une liaison automatisée [...] permettant un accès aux données contenues dans celle-ci'. et 'par interrogation directe', il faut entendre un accès direct limité 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;

d) les données relatives aux mesures à prendre pour les personnes visées au point a).'

11. L'article 13/1 de l'A.R. 12 octobre 2010 qui est proposé reprend les conditions et les modalités d'accès et d'interrogation. À cet égard, le Comité souhaite formuler les remarques suivantes.

12. Dans la première phrase du § 1er , outre l' '*accès direct*', il est également fait mention de l' '*interrogation directe*'.

13. L'A.R. doit préciser que le dirigeant du service ne peut mentionner que des personnes figurant sur la liste qui, de par leur fonction et sur la base d'un besoin manifeste, ont un droit d'accès ou d'interrogation à la base de donnée visée. Pour des considérations de protection des données, le Comité juge souhaitable, pour certaines banques de données renfermant des données très sensibles, de désigner seulement quelques personnes par l'intermédiaire desquelles les autres membres du personnel du service de renseignement pourraient adresser leurs demandes d'information motivées.

14. Dans le deuxième alinéa proposé, il est précisé que l'accès direct peut également être 'réalisé par la fourniture de fichiers de données à caractère personnel'. Le Rapport au Roi reprend à cet égard les termes suivants : 'A titre d'illustration, la DIV préfère la communication de fichiers vers un destinataire plutôt qu'une consultation dans sa banque de données, afin d'éviter une lenteur des traitements de ses propres services dans la banque de données, due à une surcharge du système'. Le Comité fait remarquer qu'à ce moment-là, il ne s'agit plus d'un accès ou d'une interrogation direct(e), mais d'une simple demande d'information, telle que prévue à l'article 14, alinéas 2 et 3 et à l'article 16, alinéa 2 L.R&S. Le Comité ne comprend d'ailleurs pas comment la

Indien deze verwerkingsverantwoordelijke een private (rechts)persoon is, zijn er in principe alleen beletsels voor advocaten, artsen en journalisten. Zij moeten hun beroeps- en bronnengeheim respecteren. Vóór de wetswijziging uit 2017, waarbij artikel 16 W.I&V gewijzigd werd, dienden private personen ook rekening te houden met het doelbindings-principe: persoonsgegevens die verwerkt waren voor doeleinde A mochten niet zondermeer doorgegeven worden aan bijvoorbeeld inlichtingendiensten die deze gegevens zouden gebruiken voor doeleinde B. Dit was zo omdat artikel 16 W.I&V oorspronkelijk expliciet verwees naar de regels inzake dataprotectie. In 2017 verviel volgende zinssnede: '*In overeenstemming met artikel 3, § 4, van de Wet van 8 december 1992, tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens*'.

Wel is het niet uitgesloten dat specifieke (reeds bestaande of nieuwe) wetten alsnog een verbod opleggen om (bepaalde) persoonsgegevens uit bepaalde databestanden door te geven aan derden, of er hen toegang tot te verlenen. Het is dus van belang dat zowel private actoren als de inlichtingendiensten onderzoeken of er een specifieke wettelijke geheimhoudings-verplichting geldt, vooraleer een toegang te verlenen.

Het Vast Comité I benadrukt opnieuw dat de mogelijkheid om rechtstreeks toegang te krijgen tot gegevensbanken niet mag gebruikt worden om wettelijke procedures die in een specifieke controle voorzien, te omzeilen. Bedoeld wordt bijvoorbeeld de rechtstreekse toegang tot lokalisatiegegevens bijgehouden door telecombedrijven of financiële gegevens verwerkt door bankinstellingen terwijl dit een specifieke of uitzonderlijke methode vormt. In deze gevallen mag geen rechtstreekse toegang of bevraging worden georganiseerd.

10. Indien bij of krachtens de wet of na akkoord van de verwerkingsverantwoordelijke een rechtstreekse toegang mogelijk wordt gemaakt, zullen minstens (in de wet, het krachtens de wet genomen besluit of het akkoord kunnen bijkomende regels geformuleerd worden) een aantal regels moeten gerespecteerd worden. Deze regels werden opgenomen in het ontwerpbesluit. Vooraf dient evenwel benadrukt dat het ontwerpbesluit niet alleen de modaliteiten voor een 'rechtstreekse toegang' maar ook voor een '*rechtstreekse bevraging*' regelt. Het ontwerp preciseert echter niet wat hieronder dient te worden begrepen. Het Comité beveelt aan dat het KB deze termen nader definieert. Daarbij kan best aansluiting gezocht worden bij de definitie zoals opgenomen in artikel 44/11/4 van de Wet op het Politieambt. '*Onder 'rechtstreekse toegang' wordt een geautomatiseerde verbinding [...] verstaan die het mogelijk maakt toegang te hebben tot de [in de databank] vervatte gegevens.*' en '*Onder 'rechtstreekse bevraging' wordt een beperkte rechtstreekse toegang tot alle of een gedeelte van de volgende gegevens verstaan:*

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;

d) de gegevens met betrekking tot de te nemen maatregelen voor de in punt a) bedoelde personen.'

11. Het voorgestelde artikel 13/1 KB 12 oktober 2010 bevat de voorwaarden en modaliteiten van de toegang en bevraging. Het Comité wenst hierbij volgende opmerkingen te formuleren.

12. In de eerste zin van § 1 dient naast de '*rechtstreekse toegang*' ook melding te worden gemaakt van de '*rechtstreekse bevraging*'.

13. Het KB dient te specifiëren dat het diensthoofd alleen personen op de lijst mag vermelden die vanuit hun functie een aantoonbare nood hebben aan een recht van toegang of bevraging van de geviseerde database. Vanuit overwegingen van dataprotectie, acht het Comité het wenselijk dat, voor bepaalde databanken waarin zeer gevoelige gegevens zijn opgenomen, slechts enkele personen zouden worden aangeduid via dewelke de andere personeelsleden van de inlichtingendienst hun vraag tot informatie op gemotiveerde wijze kunnen richten.

14. In het voorgestelde tweede lid wordt bepaald dat de rechtstreekse toegang ook kan '*gerealiseerd worden door het verschaffen van persoonsgegevensbestanden*'. In het Verslag aan de Koning wordt hierover het volgende gesteld: '*Ter illustratie: de DIV geeft veeleer de voorkeur aan de mededeling van bestanden aan een ontvanger dan aan een raadpleging van zijn gegevensbank om te voorkomen dat de verwerkingen van zijn eigen diensten in de gegevensbank traag verlopen door een overbelasting van het systeem*'. Het Comité wijst er op dat het op dat ogenblik niet meer over een rechtstreekse toegang of bevraging gaat maar over een gewone vraag tot informatie zoals bepaald in artikel 14, tweede en derde lid en artikel 16, tweede lid W.I&V. Het Comité ziet overigens niet in hoe het

réponse à de telles questions peut excéder la capacité de stockage d'un service de renseignement, à moins que la question ne porte sur l'ensemble ou sur de larges pans d'une banque de données. Dans ce cas, se posent évidemment d'autres questions de principe sur le texte proposé, comme par exemple la question de la proportionnalité et de la finalité. Dans ce cas, le service de renseignement concerné disposerait aussi d'une 'copie' d'une base de données dont les données ne seraient plus à jour, inévitablement, et seraient donc inexactes. Pour toutes ces raisons, le Comité considère qu'une forme de 'copie' n'est pas conforme aux principes fondamentaux de la protection des données.

Le Comité insiste sur l'importance de clarifier la portée du deuxième alinéa proposé et, le cas échéant, de se pencher également sur l'interrogation directe.

15. La réglementation proposée prévoit, à juste titre, la nécessité de journaliser les traitements des services de renseignement et de sécurité dans ces banques de données. Il est en outre stipulé que '*[l]es traitements des services de renseignement et de sécurité dans cette banque de données et leur journalisation sont protégés par des mesures de sécurité. Ces mesure sont mises à la disposition du Comité permanent R.*' Le Comité fait remarquer qu'il doit non seulement être informé des 'mesures' mais qu'il doit également avoir la possibilité de consulter les journalisations.

Par ailleurs, le Comité attire l'attention sur le fait que la réglementation proposée en matière de contrôle des logs d'accès par les services de renseignement dans des banques de données privées ou publiques doit remplir les conditions des articles 13 de la Loi protection des données (qui s'applique pour ainsi dire à toutes les banques de données privées et publiques) et de l'article 47 de la Loi protection des données (qui s'applique aux banques de données policières).

L'article 13 de la Loi protection des données est libellé comme suit :

'*Lorsqu'une autorité visée aux sous-titres 1er* [c'est-à-dire les services de renseignement, ndr] *et 6 du titre 3 dispose d'un accès direct ou d'une interrogation directe à une banque de données du secteur public ou du secteur privé, ses traitements de données à caractère personnel dans cette banque de données sont protégés par des mesures de sécurité techniques, organisationnelles et individuelles de sorte que seuls les acteurs suivants puissent accéder au contenu de ces traitements pour assurer leurs missions légales de contrôle :*

1° le délégué à la protection des données du responsable du traitement de la banque de données ;

2° le délégué à la protection des données de l'autorité visée aux sous-titres 1 et 6 du titre 3 ;

3° le responsable du traitement de la banque de données ou son délégué;

4° le responsable du traitement de l'autorité visée aux sous-titres 1 et 6 du titre 3 ;

5° toute autre personne précisée dans un protocole entre les responsables du traitement, pour autant que l'accès s'inscrive dans l'exercice des missions légales de contrôle des délégués à la protection des données et des responsables du traitement.

Les mesures de sécurité mentionnées à l'alinéa 1er visent à protéger les obligations légales portant sur la protection des sources, la protection de l'identité de leurs agents ou la discrétion des enquêtes des autorités visées aux sous-titres 1 et 6 du titre 3. Elles sont mises à la disposition de l'autorité de contrôle compétente.

Ces traitements ne peuvent être accessibles pour d'autres finalités que celles liées au contrôle que si ces finalités sont consignées dans un protocole d'accord par les responsables du traitement concernés parmi les finalités déterminées par ou en vertu de la loi.

Le protocole d'accord désigne la ou les personnes dont l'accès aux journaux est nécessaire pour remplir chaque finalité autorisées à l'alinéa 3.

Les journaux et les mesures de sécurité mentionnées à l'alinéa 1er sont mis à la disposition du Comité permanent R.

L'autorité visée au titre 3 concernée peut déroger à ses traitements dans une banque de données et aux journaux n'est pas susceptible de porter atteinte aux intérêts visés à l'alinéa 2.

L'article 47 de la Loi protection des données est tout à fait similaire.

16. La réglementation proposée prévoit une obligation (limitée) de journaliser également le motif justifiant l'accès direct (ou l'interrogation ?). On entend par 'obligation limitée' qu'il convient de procéder à une journalisation, selon la réglementation proposée, uniquement si c'est requis par la loi ou en vertu de celle-ci. Trop restrictif à l'estime du Comité : tout accès doit avoir une finalité légale et celle-ci doit être définie préalablement à la consultation. Comme pour certaines autres

antwoord op dergelijke vragen de opslagcapaciteit van een inlichtingendienst te boven kan gaan, tenzij de vraag betrekking zou hebben op de gehele of grote delen van een databank. In dat geval stellen zich rd andere principiële vragen bij de voorgestelde tekst, zoals bijvoorbeeld de vraag naar proportionaliteit en finaliteit. Tevens zou de betrokken inlichtingendienst in dat geval beschikken over een 'kopie' van een databank waarvan de gegevens na verloop van tijd onvermijdelijk gedateerd en dus niet accuraat zijn. Het Comité acht om al die redenen een vorm van 'kopiename' niet conform de basisprincipes van data-protectie.

Het Comité dringt er op aan de draagwijdte van het voorgestelde tweede lid te verduidelijken en desgevallend ook de situatie van de rechtstreekse bevraging te behandelen.

15. De voorgestelde regeling voorziet er terecht in dat de verwerkingen van de inlichtingen- en veiligheidsdiensten in deze gegevensbanken moeten worden gelogd. Verder wordt bepaald dat '*[d]e verwerkingen van de inlichtingen- en veiligheidsdiensten en de logbestanden ervan worden beschermd door beveiligings-maatregelen. Deze maatregelen worden ter beschikking gesteld van het Vast Comité I.*' Het Comité wijst er op dat het niet alleen in kennis moet worden gesteld van de 'maatregelen' maar ook over de mogelijkheid moet kunnen beschikken om de logbestanden zelf te raadplegen.

Verder wijst het Comité er op dat de voorgestelde regeling inzake controle van logs van de toegang door inlichtingendiensten in private of publieke databanken moet voldoen aan artikelen 13 Gegevensbeschermingswet (dat van toepassing is op omzeggens alle private en publieke databanken) en artikel 47 Gegevensbeschermingswet (dat van toepassing is op politionele databanken).

Artikel 13 Gegevensbeschermingswet luidt als volgt:

'*Wanneer een overheid bedoeld in ondertitels 1* [zijnde de inlichtingendiensten, nvda] *en 6 van titel 3 over een rechtstreekse toegang of over een rechtstreekse bevraging van een gegevensbank van de openbare of private sector beschikt, worden zijn verwerkingen van persoonsgegevens in deze gegevensbank beschermd door technische, organisatorische en individuele beveiligingsmaatregelen zodat alleen de volgende actoren toegang kunnen hebben tot de inhoud van deze verwerkingen om hun wettelijke toezichtsopdrachten uit te voeren:*

1° de functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke van de gegevensbank;

2° de functionaris voor gegevensbescherming van de overheid bedoeld in de ondertitels 1 en 6 van titel 3;

3° de verwerkingsverantwoordelijke van de gegevensbank of zijn gemachtigde;

4° de verwerkingsverantwoordelijke van de overheid bedoeld in de ondertitels 1 en 6 van titel 3;

5° elke andere persoon bepaald in een protocol tussen de verwerkingsverantwoordelijken voor zover de toegang past in de uitvoering van de wettelijke toezichtsopdrachten van de functionarissen voor gegevensbescherming en de verwerkingsverantwoordelijken.

De in het eerste lid vermelde beveiligingsmaatregelen zijn bedoeld om de wettelijke verplichtingen met betrekking tot de bescherming van bronnen, de bescherming van de identiteit van de agenten of de discretie van de onderzoeken van de overheden bedoeld in ondertitels 1 en 6 van titel 3 te beschermen. Zij worden ter beschikking gesteld van de bevoegde toezichthoudende autoriteit.

Deze verwerkingen mogen enkel toegankelijk zijn voor andere doeleinden dan deze die verband houden met het toezicht indien deze doeleinden vastgelegd zijn in een protocolakkoord door de betrokken verwerkingsverantwoordelijken binnen de doeleinden voorzien door of krachtens een wet.

Het protocolakkoord duidt de persoon of personen aan waarvoor de toegang tot de logbestanden noodzakelijk is ter vervulling van elke doeleinde toegelaten in het derde lid.

De logbestanden en de in het eerste lid vermelde beveiligingsmaatregelen worden ter beschikking gesteld van het Vast Comité I.

De betrokken overheid bedoeld in titel 3 kan afwijken van het eerste lid wanneer de toegang tot zijn verwerkingen in een gegevensbank en de logbestanden geen afbreuk kan doen aan de belangen bedoeld in het tweede lid'.

Artikel 47 Gegevensbeschermingswet is volledig gelijkaardig.

16. De voorgestelde regeling voorziet in een (beperkte) verplichting om de reden die de rechtstreekse toegang (of bevraging?) rechtvaardigen ook te loggen. De beperking bestaat erin dat dit blijkens de voorgestelde regeling alleen moet indien dit door of krachtens de wet vereist is. Het Comité is van oordeel dat dit te beperkt is: elke toegang moet een wettelijke finaliteit hebben en deze dient voorafgaand aan de consultatie vast te staan. Net zoals voor bepaalde andere gewone

méthodes ordinaires, l'accès direct doit être suffisamment motivé ; une simple mention de la menace ne suffit pas. Le Comité observe que les articles 14 et 16 L.R&S offrent potentiellement un accès à pratiquement toutes les banques de données existantes, qu'elles soient publiques ou privées (à l'exception des banques de données qui tombent sous le régime d'une méthode spécifique ou exceptionnelle), un tel accès pouvant se révéler très intrusif. Cet accès aux banques de données n'est pas soumis à un contrôle a priori ; seul un contrôle ex ante du Comité est possible. Pour rendre ce contrôle efficace, le motif de tout accès direct doit être journalisé, ne serait-ce que de manière sommaire.

17. L'article proposé précise ce qui suit : '*Par dérogation à l'alinéa précèdent, la journalisation et les raisons justifiant le traitement peuvent être enregistrées en dehors du service de renseignement et de sécurité, lorsque le dirigeant du service concerné estime que cet enregistrement n'est pas susceptible de porter atteinte à la protection des sources, à la protection de l'identité des agents et à la discrétion des enquêtes de renseignement*'. Le Comité s'interroge sur la raison d'être de cette réglementation. Et de souligner que quiconque sauvegarde de telles données pour les services de renseignement doit être considéré comme un 'sous-traitant' au sens de la Loi protection des données, avec toutes les conséquences que cela implique en termes juridiques (voir par ex. les articles 84 et suiv.).

18. L'article 3 § 2 de l'A.R. du 12 octobre 2010 porte sur la situation où '*un accès direct aux banques de données qui contiennent des données à caractère personnel est impossible*'. Le Comité demande un complément d'information sur cette impossibilité. S'agit-il d'une simple impossibilité technique et temporaire ? Le Comité considère que dans cette situation-là aussi, il est nécessaire de conserver les journaux de toutes les demandes formulées par les agents.

Toujours en ce qui concerne cette disposition, le Comité fait remarquer que selon toute vraisemblance, il faut également mentionner l'impossibilité d''*interrogation directe*'.

19. Le Rapport au Roi mentionne ce qui suit : '*Si la raison du traitement doit également être enregistrée, il est alors prévu que cette raison et le traitement lui-même soient enregistrés au sein du service de renseignement concerné (et non au sein de la banque de données). Cela se justifie par la nécessité de protéger notamment les sources, les agents ainsi que la discrétion des enquêtes de renseignement. En outre, la raison du traitement est la plupart du temps classifiée au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, elle ne peut donc être conservée que sur un réseau classifié*'. Le Comité comprend parfaitement cette préoccupation mais attire l'attention sur les articles 13 et 47 précités de la Loi protection des données, qui octroient une mission de contrôle au responsable du traitement et au fonctionnaire de la protection des données de la banque de données concernée. Le Comité permanent R attire l'attention sur le fait que le projet d'arrêté doit respecter cette obligation.

Accès à la BNG

20. Le Comité attire l'attention sur le fait que les services de renseignement n'ont toujours pas (d') accès (direct) à la Banque de données Nationale Générale de la police, et ce malgré la recommandation de la Commission d'enquête parlementaire Attentats visant à optimaliser le flux d'informations. Cependant, tant sur la base de l'article 14, alinéa 4 L.R&S que sur la base de l'article 44/11/12 § 1er, 2° Loi sur la fonction de police, un accès/une interrogation directe peut être rendu(e) possible.

La proposition de loi modifiant diverses dispositions en ce qui concerne la gestion de l'information policière (doc 54 3697/001) constitue une nouvelle tentative pour octroyer un accès direct des services de renseignement à la BNG. L'entrée en vigueur de cette disposition a toutefois été conditionnée à la conclusion d'un accord régissant également le flux d'informations inverse. Le Comité permanent R déplore, d'une part, de ne pas avoir été sollicité pour rendre un avis sur cette réglementation cruciale, et d'autre part, émet de sérieuses réserves quant à la 'réciprocité' proposée.

La désignation du fonctionnaire en matière de protection des données

21. L'article 13/1 de l'A.R. du 12 octobre 2010 qui est proposé dispose que le 'ministre compétent' (c'est-à-dire le ministre de la Justice en ce qui concerne la Sûreté de l'État et le ministre de la Défense en ce qui concerne le Service Général du Renseignement et de la Sécurité), après avis du dirigeant du service, procède à la désignation du fonctionnaire.

De cette manière, l'A.R. part du principe que le ministre est le responsable du traitement pour les traitements qui sont effectués par le service renseignement qui relève de sa compétence (art. 72 2° Loi protection des données). Le Comité permanent R souscrit à ce principe.

methoden, moet de rechtstreekse toegang afdoende gemotiveerd worden en daarbij volstaat een loutere verwijzing naar een dreiging niet. Het Comité wijst er op dat de artikelen 14 en 16 W.I&V een potentiële toegang bieden tot quasi alle publieke en private bestaande databanken (met uitzondering van de databanken die onder het regime van een specifieke of uitzonderlijke methode vallen) en op die wijze potentieel zeer intrusief zijn. De toegang tot de databanken is niet onderworpen aan een a priori-controle; er is alleen een mogelijke ex ante-controle door het Comité. Om deze controle effectief te maken moet de reden van elke rechtstreekse toegang, weze het op een summiere wijze, gelogd worden.

17. Het ontworpen artikel bepaalt verder het volgende: '*In afwijking van het voorgaande lid mogen de logbestanden en de redenen die de verwerking rechtvaardigen opgeslagen worden buiten de inlichtingen- en veiligheidsdienst, wanneer het betrokken diensthoofd van oordeel is dat deze opslag geen afbreuk kan doen aan de bescherming van de bronnen, aan de bescherming van de identiteit van de agenten en aan de discretie van de inlichtingenonderzoeken*'. Het Comité stelt zich vragen bij het waarom van deze regeling. Het wijst er verder op dat diegene die voor de inlichtingendiensten dergelijke gegevens opslagen als 'verwerker' moeten worden beschouwd in de zin van de Gegevensbeschermingswet met alle juridische consequenties dat dit met zich brengt (zie bijv. artt. 84 e.v.).

18. Artikel 3 § 2 KB 12 oktober 2010 handelt over de situatie waarbij '*de rechtstreekse toegang tot de gegevensbanken die persoonsgegevens bevatten onmogelijk is*'. Het Comité vraagt om nader toe te lichten waaruit deze onmogelijkheid bestaat. Betreft het een louter technische en tijdelijke onmogelijkheid? Het Comité is van oordeel dat ook in deze situatie logs dienen bijgehouden te worden van de aanvragen die agenten formuleren.

Nog wat betreft deze bepaling merkt het Comité op dat naar alle waarschijnlijkheid ook melding dient te worden gemaakt van de onmogelijkheid tot de '*rechtstreekse bevraging*'.

19. Het Verslag aan de Koning vermeldt het volgende: '*Indien de reden voor de verwerking eveneens geregistreerd moet worden, wordt voorzien dat deze reden en de verwerking zelf dan geregistreerd worden binnen de betrokken inlichtingendienst (en niet binnen de gegevensbank). Dit wordt gerechtvaardigd door de noodzaak om met name de bronnen, de agenten en de discretie van de inlichtingenonderzoeken te beschermen. Bovendien wordt de reden voor de verwerking meestal geclassificeerd in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen. Zij kan dan ook enkel op een geclassificeerd netwerk worden bewaard*.' Het Comité heeft ten volle begrip voor deze bekommernis maar wijst op bovenstaande artikelen 13 en 47 Gegevensbeschermingswet die aan de verwerkingsverantwoordelijke en de functionaris voor de gegevensbescherming van de betrokken databank een toezichtopdracht toevertrouwen. Het Vast Comité I wijst er op dat het ontwerpbesluit deze verplichting moet respecteren.

Toegang tot de ANG

20. Het Comité merkt op dat de inlichtingendiensten tot op heden nog geen (rechtstreekse) toegang hebben tot de Algemene Nationale Gegevensbank van de politie, dit ondanks de aanbeveling van de Parlementaire onderzoekscommissie Aanslagen om tot een optimale informatiedoorstroming te komen. Nochtans zou zowel op basis van artikel 14, vierde lid W.I&V als op basis van artikel 44/11/12 § 1, 2° Wet op het Politieambt een toegang/rechtstreekse bevraging mogelijk kunnen gemaakt worden.

Bij Wetsvoorstel tot wijziging van diverse bepalingen wat het politionele informatiebeheer betreft (doc 54 3697/001) wordt opnieuw een poging ondernomen om de inlichtingendiensten een rechtstreekse toegang te verlenen tot de ANG. De inwerkingtreding van deze bepaling wordt echter afhankelijk gesteld van het sluiten van een akkoord waarbij ook de omgekeerde informatiestroom wordt geregeld. Het Vast Comité I betreurt enerzijds dat het niet om advies werd gevraagd met betrekking tot deze cruciale regeling, en maakt anderzijds ernstig voorbehoud bij de voorgestelde 'weder-kerigheid'.

De aanduiding van de functionaris inzake gegevensbescherming

21. Het voorgestelde artikel 13/1 KB 12 oktober 2010 stelt dat de 'bevoegde minister' (met andere woorden de minister van Justitie wat betreft de Veiligheid van de Staat en de minister van Defensie wat betreft de Algemene Dienst Inlichting en Veiligheid), na advies van het diensthoofd de functionaris aanduidt.

Op die wijze gaat het KB er van uit dat de minister de verwerkingsverantwoordelijke is voor de verwerkingen die gebeuren door de inlichtingendienst die tot zijn bevoegdheid behoort (art. 72 2° Gegevensbeschermingswet). Het Vast Comité I kan zich hier in vinden. Het

De fait, le ministre de la Justice et le ministre de l'Intérieur sont les responsables du traitement pour le traitement des données à caractère personnel respectivement en matière de police judiciaire et de police administrative.

La communication structurée de la Commission BIM

22. Le projet propose de supprimer la communication structurée établie par la Commission BIM concernant chaque méthode (art. 11 alinéa 4 AR 12 octobre 2010) '[c]es mentions ayant été reprises aux articles 18/3 et 18 /10 de la loi du 30 novembre 1998'.

Le Comité permanent R fait néanmoins remarquer que la communication structurée reprend quelques données complémentaires qui sont pertinentes pour son contrôle : le moment où la décision de la Commission BIM est communiquée (ce n'est qu'à ce moment-là qu'une méthode spécifique peut être mise en œuvre) et le fait que la décision, l'autorisation ou l'avis porte sur une prolongation.

Le Comité préconise dès lors de conserver une communication structurée et d'ajouter les éléments énumérés aux articles 18/3 et 18/10 L.R&S.

Bruxelles, le 9 avril 2019.

POUR LE COMITÉ PERMANENT R
Serge LIPSZYC
Président
Wouter DE RIDDER
Greffier

CONSEIL D'ÉTAT
section de législation
avis 65.640/2 du 9 avril 2019

Sur un projet d'arrêté royal 'modifiant l'arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'arrêté royal du 3 juillet 2016 portant exécution de l'article 21 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité'

Le 11 mars 2019, le Conseil d'État, section de législation, a été invité par le Ministre de la Justice, chargé de la Régie des bâtiments à communiquer un avis, dans un délai de trente jours, sur un projet d'arrêté royal 'modifiant l'arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'arrêté royal du 3 juillet 2016 portant exécution de l'article 21 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité'.

Le projet a été examiné par la deuxième chambre le 9 avril 2019. La chambre était composée de Pierre VANDERNOOT, président de chambre, Wanda VOGEL et Patrick RONVAUX, conseillers d'État, Marianne DONY, assesseur, et Béatrice DRAPIER, greffier.

Le rapport a été présenté par Xavier DELGRANGE, premier auditeur chef de section.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Pierre VANDERNOOT.

L'avis, dont le texte suit, a été donné le 9 avril 2019.

*

Compte tenu du moment où le présent avis est donné, le Conseil d'État attire l'attention sur le fait qu'en raison de la démission du Gouvernement, la compétence de celui ci se trouve limitée à l'expédition des affaires courantes. Le présent avis est toutefois donné sans qu'il soit examiné si le projet relève bien de la compétence ainsi limitée, la section de législation n'ayant pas connaissance de l'ensemble des éléments de fait que le Gouvernement peut prendre en considération lorsqu'il doit apprécier la nécessité d'arrêter ou de modifier des dispositions réglementaires.

Comme la demande d'avis est introduite sur la base de l'article 84, § 1er, alinéa 1er, 2°, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, la section de législation limite son examen au fondement juridique du 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, le projet appelle les observations suivantes.

is immers ook zo dat de minister van Justitie en de minister van Binnenlandse Zaken de verwerkingsverantwoordelijken zijn voor de verwerkingen van persoonsgegevens inzake respectievelijk gerechtelijke en administratieve politie.

De gestructureerde mededeling van de BIM-Commissie

22. Het ontwerp stelt voor de gestructureerde mededeling die de BIM-Commissie opstelt naar aanleiding van elke methode te schrappen (art. 11 lid 4 KB 12 oktober 2010) *'[a]angezien deze vermeldingen in artikelen 18/3 en 18/10 van de wet van 30 november 1998 opgenomen werden'*.

Het Vast Comité I merkt echter op dat de gestructureerde mededeling enkele bijkomende gegevens bevat die relevant zijn voor zijn controle: het moment van de kennisgeving van de beslissing aan de BIM-Commissie (pas vanaf dan mag een specifieke methode worden uitgevoerd) en het feit of de beslissing, de machtiging of het advies betrekking heeft op een verlenging.

Het Comité pleit er dan ook voor de gestructureerde mededeling te behouden en aan te vullen met de elementen opgesomd in de artikelen 18/3 en 18/10 W.I&V.

Brussel, 9 april 2019.

VOOR HET VAST COMITÉ I
Serge LIPSZYC
Voorzitter
Wouter DE RIDDER
Griffier

RAAD VAN STATE
afdeling Wetgeving
advies 65.640/2 van 9 april 2019

Over een ontwerp van koninklijk besluit 'tot wijziging van het koninklijk besluit houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen en veiligheidsdiensten en het koninklijk besluit van 3 juli 2016 houdende uitvoering van artikel 21 van de wet van 30 november 1998 houdende regeling van de inlichtingen en veiligheidsdienst'

Op 11 maart 2019 is de Raad van State, afdeling Wetgeving, door de Minister van Justitie, belast met de Regie der gebouwen verzocht binnen een termijn van dertig dagen een advies te verstrekken over een ontwerp van koninklijk besluit 'tot wijziging van het koninklijk besluit houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en het koninklijk besluit van 3 juli 2016 houdende uitvoering van artikel 21 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst'.

Het ontwerp is door de tweede kamer onderzocht op 9 april 2019. De kamer was samengesteld uit Pierre VANDERNOOT, kamervoorzitter, Wanda VOGEL en Patrick RONVAUX, staatsraden, Marianne DONY, assessor, en Béatrice DRAPIER, griffier.

Het verslag is uitgebracht door Xavier DELGRANGE, eerste auditeur-afdelingshoofd.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Pierre VANDERNOOT.

Het advies, waarvan de tekst hierna volgt, is gegeven op 9 april 2019.

*

Rekening houdend met het tijdstip waarop dit advies gegeven wordt, vestigt de Raad van State de aandacht op het feit dat, wegens het ontslag van de regering, de bevoegdheid van deze laatste beperkt is tot het afhandelen van de lopende zaken. Dit advies wordt evenwel gegeven zonder dat wordt nagegaan of het ontwerp onder die beperkte bevoegdheid valt, aangezien de afdeling Wetgeving geen kennis heeft van alle feitelijke gegevens die de regering in aanmerking kan nemen als zij moet beoordelen of het nodig is een verordening vast te stellen of te wijzigen.

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 ontwerp, de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

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

FORMALITÉS PRÉALABLES

L'article 36, paragraphe 4, du règlement (UE) n° 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 n° 95/46/CE (règlement général sur la protection des données)' combiné avec l'article 57, paragraphe 1, *c)*, et le considérant 96 de ce règlement, impose de consulter l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement.

En outre, comme le relève son commentaire, l'article 6 du projet, qui modifie l'article 3 de l'arrêté royal du 12 octobre 2010 'portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité', exécute notamment l'article 16/4 de la loi du 30 novembre 1998 'organique des services de renseignement et de sécurité', inséré par la loi du 21 mars 2018. L'habilitation figurant dans cet article gît dans son paragraphe 1er, alinéa 1er, rédigé comme suit :

« Selon les modalités déterminées par le Roi, après avis de l'autorité compétente de contrôle des traitements de données à caractère personnel, un accès direct est autorisé pour les services de renseignement et de sécurité aux informations et données à caractère personnel qui sont collectées au moyen de caméras dont l'utilisation par les services de police est autorisée conformément au chapitre IV, section 1re, et au chapitre IV/1, section 2, de la loi sur la fonction de police et qui sont notamment traitées dans les banques de données visées à l'article 44/2 de ladite loi ».

L'autorité compétente de contrôle des traitements de données à caractère personnel par les services de renseignement et de sécurité et par leurs sous-traitants est, conformément à l'article 95 de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel', le Comité permanent R.

Il ne résulte pas du dossier que cet avis a été rendu.

EXAMEN DU PROJET

PRÉAMBULE

1. À l'alinéa 2, les différents articles de la loi du 30 novembre 1998 'organique des services de renseignement et de sécurité' servant de fondement juridique au projet seront cités dans leur ordre chronologique, en mentionnant, pour chaque article ou subdivision d'article éventuelle, les modifications encore en vigueur que cet article ou cette subdivision a subies (1).

Il convient en outre d'ajouter la mention de l'article 27, alinéa 4, de la loi du 30 novembre 1998, qui sert de fondement juridique à l'article 16 du projet, et de remplacer les mots « 43/4, § 1er » par les mots « 43/4, alinéa 1er ».

2. La loi du 3 décembre 2017 'portant création de l'Autorité de protection des données' ne procurant pas de fondement juridique à l'arrêté en projet, l'alinéa 3 du préambule sera omis.

3. À l'alinéa 4, il y a lieu d'omettre la mention de l'article 95 de la loi du 30 juillet 2018 'relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel', cette disposition ne procurant pas de fondement juridique à l'arrêté en projet.

4. Le préambule sera complété par deux alinéas, dans lesquels seront visés respectivement l'arrêté royal du 12 octobre 2010 'portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité' et l'arrêté royal du 3 juillet 2016 'portant exécution de l'article 21 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité', qui sont tous deux modifiés par l'arrêté en projet (2).

OBSERVATION FINALE

Il est contraire aux règles de légistique de renuméroter des articles ou d'autres divisions du dispositif (3) .

VOORAFGAANDE VORMVEREISTEN

Volgens artikel 36, lid 4, van verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 'betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)', in combinatie met artikel 57, lid 1, *c)*, en met overweging 96 van die verordening, moet de toezichthoudende autoriteit geraadpleegd worden wanneer een door een nationaal parlement vast te stellen voorstel voor een wetgevingsmaatregel of een daarop gebaseerde regelgevingsmaatregel in verband met verwerking wordt opgesteld.

Voorts wordt in de toelichting van het ontwerp opgemerkt dat artikel 6 van het ontwerp, waarbij artikel 3 van het koninklijk besluit van 12 oktober 2010 'houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten' wordt gewijzigd, onder meer uitvoering geeft aan artikel 16/4 van de wet van 30 november 1998 'houdende regeling van de inlichtingen- en veiligheidsdiensten', dat bij de wet van 21 maart 2018 is ingevoegd. De machtiging die in dat artikel wordt gegeven, steunt op het eerste lid van paragraaf 1 ervan en luidt als volgt:

"Overeenkomstig de nadere regels bepaald door de Koning, na advies van de bevoegde toezichthoudende autoriteit voor de verwerking van persoonsgegevens, is een rechtstreekse toegang toegestaan voor de inlichtingen- en veiligheidsdiensten tot de informatie en persoonsgegevens die verzameld worden door middel van camera's waarvan het gebruik door de politiediensten is toegestaan overeenkomstig hoofdstuk IV, afdeling 1, en hoofdstuk IV/1, afdeling 2, van de wet op het politieambt en die in het bijzonder worden verwerkt in de gegevensbanken bedoeld in artikel 44/2 van de genoemde wet."

Overeenkomstig artikel 95 van de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens' is het Vast Comité I de bevoegde autoriteit die toezicht houdt op de verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten en door hun verwerkers.

Uit het dossier blijkt niet dat dat advies gegeven is.

ONDERZOEK VAN HET ONTWERP

AANHEF

1. In het tweede lid moeten de verschillende artikelen van de wet van 30 november 1998 'houdende regeling van de inlichtingen- en veiligheidsdiensten' die als rechtsgrond dienen voor het ontwerp, in chronologische volgorde worden vermeld, en moeten voor elk artikel of elke eventuele onderverdeling ervan de nog geldende wijzigingen worden opgegeven die in dat artikel of in die onderverdeling zijn aangebracht (1).

Voorts moet eveneens melding worden gemaakt van artikel 27, vierde lid, van de wet van 30 november 1998, dat rechtsgrond biedt voor artikel 16 van het ontwerp, en moeten in de Franse tekst de woorden "43/4, § 1er" worden vervangen door de woorden "43/4, alinéa 1er".

2. Het derde lid van de aanhef moet worden weggelaten, aangezien de wet van 3 december 2017 'tot oprichting van de Gegevensbeschermingsautoriteit' het ontworpen besluit geen rechtsgrond verleent.

3. In het vierde lid hoort artikel 95 van de wet van 30 juli 2018 'betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens' niet te worden vermeld omdat het geen rechtsgrond verleent aan het ontworpen besluit.

4. Aan de aanhef moeten twee leden worden toegevoegd, waarin wordt verwezen naar respectievelijk het koninklijk besluit van 12 oktober 2010 'houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten' en het koninklijk besluit van 3 juli 2016 'houdende uitvoering van artikel 21 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst'. Die beide besluiten worden door het ontworpen besluit gewijzigd. (2)

SLOTOPMERKING

Het is strijdig met de wetgevingstechnische regels om artikelen of andere indelingen van het dispositief te vernummeren (3).

Les articles 8, 2°, 3° et 5°, 15, 16, 17 et 18 seront revus en conséquence.

LE GREFFIER — LE PRÉSIDENT
Béatrice DRAPIER — Pierre VANDERNOOT

Notes

(1) Principes de technique législative - Guide de rédaction des textes législatifs et réglementaires, www.raadvst consetat.be, onglet « Technique législative », recommandation n° 27, *b)* et *c)*, et formules F 3 2 2 à F 3 2 8.

(2) Ibid., recommandation n° 30 et formule F 3 3.

(3) Ibid., recommandation n° 125.

2 OCTOBRE 2019. — Arrêté royal modifiant l'arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'arrêté royal du 3 juillet 2016 portant exécution de l'article 21 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

PHILIPPE, Roi des Belges,
A tous, présents et à venir, Salut.

Vu la Constitution, l'article 108 ;

Vu la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, les articles 13/2 et 13/3 insérés par la loi du 30 mars 2017 modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259*bis* du Code pénal, l'article 14, alinéa 4, inséré par la loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité, l'article 16/4 inséré par la loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, l'article 18/3, § 6, alinéa 3, inséré par la loi du 4 février 2010 précitée, l'article 18/10, § 4, alinéa 5, modifié par la loi du 30 mars 2017 précitée, l'article 18/10, § 6, alinéa 4, inséré par la loi du 4 février 2010 précitée, l'article 18/17, § 7, modifié par la loi du 30 mars 2017 précitée , l'article 21, l'article 27, alinéa 4, inséré par la loi du 30 mars 2017 précitée, l'article 43/3, modifié par la loi du 30 mars 2017 précitée, l'article 43/4, alinéa 1er, inséré par la loi du 4 février 2010 précitée et l'article 43/6, modifié par la loi du 30 mars 2017 précitée ;

Vu la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel, les articles 91 et 253 ;

Vu l'arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ;

Vu l'arrêté royal du 3 juillet 2016 portant exécution de l'article 21 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ;

Vu l'avis de l'Inspecteur des Finances accrédité auprès du ministre de la Justice, donné le 3 janvier 2019 ;

Vu l'avis de l'Inspecteur des Finances accrédité auprès du ministre de la Défense, donné le 6 décembre 2018 ;

Vu l'accord du ministre du Budget, donné le 11 février 2019 ;

Vu l'avis n° 002/CPR-ACC/2019 du Comité permanent de contrôle des services de renseignement et de sécurité, donné le 9 avril 2019;

De artikelen 8, 2°, 3° en 5°, 15, 16, 17 en 18 moeten dienovereenkomstig worden herzien.

DE GRIFFIER — DE VOORZITTER
Béatrice DRAPIER — Pierre VANDERNOOT

Nota's

(1) Beginselen van de wetgevingstechniek - Handleiding voor het opstellen van wetgevende en reglementaire teksten, www.raadvst-consetat.be, tab "Wetgevingstechniek", aanbeveling 27, *b)* en *c)*, en formules F 3 2 2 tot F 3 2 8.

(2) Ibid., aanbeveling 30 en formule F 3-3.

(3) Ibit., aanbeveling 125.

2 OKTOBER 2019. — Koninklijk besluit tot wijziging van het koninklijk besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en het koninklijk besluit van 3 juli 2016 houdende uitvoering van artikel 21 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst

FILIP, Koning der Belgen,
Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Gelet op de Grondwet, het artikel 108;

Gelet op de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, de artikelen 13/2 en 13/3 ingevoegd bij de voornoemde wet van 30 maart 2017 tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en van artikel 259*bis* van het Strafwetboek, het artikel 14, vierde lid, ingevoegd bij de wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten, het artikel 16/4 ingevoegd bij 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, het artikel 18/3, § 6, derde lid, ingevoegd bij de voornoemde wet van 4 februari 2010, het artikel 18/10, § 4, vijfde lid, gewijzigd door de voornoemde wet van 30 maart 2017, het artikel 18/10, § 6, vierde lid, ingevoegd bij de voornoemde wet van 4 februari 2010, het artikel 18/17, § 7, gewijzigd door de voornoemde wet van 30 maart 2017, het artikel 43/3, gewijzigd door de voornoemde wet van 30 maart 2017, het artikel 43/4, eerste lid, ingevoegd bij de voornoemde wet van 4 februari 2010 en het artikel 43/6, gewijzigd door de voornoemde wet van 30 maart 2017 ;

Gelet op de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, de artikelen 91 en 253;

Gelet op het koninklijk besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten ;

Gelet op het koninklijk besluit van 3 juli 2016 houdende uitvoering van artikel 21 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst ;

Gelet op het advies van de Inspecteur van Financiën geaccrediteerd bij de minister van Justitie, gegeven op 3 januari 2019;

Gelet op het advies van de Inspecteur van Financiën geaccrediteerd bij de minister van Defensie, gegeven op 6 december 2018;

Gelet op de akkoordbevinding van de minister voor Begroting, gegeven op 11 februari 2019;

Gelet op het advies nr. 002/CPR-ACC/2019 van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, gegeven op 9 april 2019;

Vu l'avis n° 65.640/2 du Conseil d'Etat, donné le 9 avril 2019, en application de l'article 84, § 1er, alinéa 1er, 2°, des lois sur le Conseil d'Etat, coordonnées le 12 janvier 1973;

Sur la proposition du Ministre de la Justice et du Ministre de la Défense,

Nous avons arrêté et arrêtons :

CHAPITRE I. — *Modification de l'arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité*

Article 1er. Dans l'article 1er de l'arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, le 3° est remplacé par ce qui suit :

« 3° « loi du 30 juillet 2018 » : la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. »

Art. 2. Dans le même arrêté, l'intitulé du chapitre II est remplacé par ce qui suit :

« Chapitre II. - Mesures de protection et d'appui ».

Art. 3. A l'article 2 du même arrêté, les modifications suivantes sont apportées :

1° à l'alinéa 1er, les mots « article 13/1, § 1er » sont remplacés par les mots « article 13/2, le mot « listes » est remplacé par le mot « registres » et les mots « , identités et qualités fictives » sont insérés entre les mots « faux noms » et le mot « indiquant » ;

2° à l'alinéa 2, les mots « de l'identité fictive et/ou de la qualité fictive, » sont ajoutés entre les mots « faux nom, » et les mots « les dates » ;

3° l'article est complété par deux alinéas rédigés comme suit :

« Le dirigeant du service concerné, ou la personne qu'il désigne à cet effet, est informé par écrit tous les deux mois de l'utilisation des identités et qualités fictives.

Le journal de bord, visé à l'alinéa 2, est conservé au minimum pendant dix ans après la dernière utilisation du faux nom, de l'identité ou de la qualité fictive. »

Art. 4. Dans le même arrêté, il est inséré un nouvel article rédigé comme suit :

« Art. 2/1. En application de l'article 13/3 de la loi du 30 novembre 1998, le dirigeant du service de renseignement et de sécurité concerné, ou son délégué, peut décider par écrit de créer une personne morale dans l'intérêt de l'exercice de ses missions. La personne qu'il désigne à cet effet tient un registre des personnes morales créées indiquant la ou les personne(s) qui en sont responsables.

La personne responsable de la personne morale enregistre dans un journal de bord l'utilisation de celle-ci, les dates, le contexte et, le cas échéant, les incidents survenus.

Le dirigeant du service concerné, ou la personne qu'il désigne à cet effet, est informé par écrit tous les deux mois de l'utilisation visée à l'alinéa 2.

Le journal de bord, visé à l'alinéa 2, est conservé au minimum pendant dix ans après la dissolution ou la liquidation de la personne morale. ».

Art. 5. Dans le même arrêté, l'intitulé du chapitre III est remplacé par ce qui suit :

« Chapitre III. - Des méthodes ordinaires de recueil des données - Accès aux banques de données externes ».

Art. 6. A l'article 3, § 1er, du même arrêté, les modifications suivantes sont apportées :

1° A l'alinéa 1er, les mots « Pour l'application de l'article 14, alinéa 4, de la loi du 30 novembre 1998, » sont abrogés ;

2° au même alinéa, les mots « peuvent disposer d'un accès direct à une banque de données du secteur public » sont remplacés par les mots « disposent d'un accès direct dans une banque de données externe » ;

3° au même alinéa, les mots « de la Commission de la protection de la vie privée » sont remplacés par les mots « du Comité permanent R » ;

Gelet op advies nr. 65.640/2 van de Raad van State, gegeven op 9 april 2019 met toepassing van artikel 84, § 1, eerste lid, 2°, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973;

Op de voordracht van de Minister van Justitie en de Minister van Defensie,

Hebben Wij besloten en besluiten Wij :

HOOFDSTUK I. — *Wijzigingen aan het koninklijk besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten*

Artikel 1. In artikel 1 van het koninklijk besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, wordt de bepaling onder 3° vervangen als volgt:

"3° "wet van 30 juli 2018" : de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens."

Art. 2. In hetzelfde besluit wordt het opschrift van hoofdstuk II vervangen als volgt:

"Hoofdstuk II. – Beschermings- en ondersteuningsmaatregelen."

Art. 3. In artikel 2 van hetzelfde besluit worden de volgende wijzigingen aangebracht :

1° in het eerste lid worden de woorden "artikel 13/1, § 1" vervangen door de woorden "artikel 13/2", wordt het woord "lijsten" vervangen door het woord "registers" en worden de woorden ", fictieve identiteiten en hoedanigheden" ingevoegd tussen de woorden "valse namen" en het woord "die";

2° in het tweede lid worden de woorden "van de fictieve identiteit en/of van de fictieve hoedanigheid" ingevoegd tussen de woorden "van de valse naam," en de woorden "de data";

3° het artikel wordt aangevuld met de volgende twee leden, luidend als volgt:

"Het betrokken diensthoofd of de persoon die hij hiertoe aanstelt, wordt om de twee maanden schriftelijk op de hoogte gesteld van het gebruik van de fictieve identiteiten en hoedanigheden.

Het logboek, bedoeld in het tweede lid, wordt bewaard gedurende minstens tien jaar na het laatste gebruik van de valse naam, van de fictieve identiteit of van de fictieve hoedanigheid."

Art. 4. In hetzelfde besluit wordt een nieuw artikel ingevoegd, luidend als volgt:

"Art. 2/1. In toepassing van artikel 13/3 van de wet van 30 november 1998, kan het hoofd van de betrokken inlichtingen- en veiligheidsdienst of zijn gedelegeerde, schriftelijk beslissen om een rechtspersoon op te richten in het belang van de uitoefening van zijn opdrachten. De persoon die hij hiertoe aanstelt houdt een register van de opgerichte rechtspersonen bij, met aanduiding van de persoon of personen die hiervoor aansprakelijk zijn.

De persoon die aansprakelijk is voor de rechtspersoon registreert in een logboek het gebruik ervan, de data, de context en eventuele incidenten die zich hebben voorgedaan.

Het betrokken diensthoofd of de persoon die hij hiertoe aanstelt, wordt om de twee maanden schriftelijk op de hoogte gesteld van het gebruik bedoeld in het tweede lid.

Het logboek, bedoeld in het tweede lid, wordt bewaard gedurende minstens tien jaar na de ontbinding of vereffening van de rechtspersoon. ".

Art. 5. In hetzelfde besluit wordt het opschrift van hoofdstuk III vervangen als volgt:

"Hoofdstuk III. – Gewone methoden voor het verzamelen van gegevens – Toegang tot externe gegevensbanken."

Art. 6. In artikel 3, § 1, van hetzelfde besluit worden de volgende wijzigingen aangebracht:

1° in het eerste lid worden de woorden "Voor de toepassing van artikel 14, vierde lid, van de wet van 30 november 1998," opgeheven;

2° in hetzelfde lid worden de woorden "kunnen beschikken over rechtstreekse toegang tot een gegevensbank van de openbare sector" vervangen door de woorden "beschikken over een rechtstreekse toegang tot een externe gegevensbank";

3° in hetzelfde lid worden de woorden "de Commissie voor de bescherming van de persoonlijke levenssfeer" vervangen door de woorden "het Vast Comité I";

4° au même alinéa, les mots « la banque » sont remplacés par « cette banque » ;

5° cinq alinéas sont insérés entre le premier et le deuxième alinéa, rédigés comme suit :

« Sauf si la capacité d'enregistrement du service de renseignement et de sécurité concerné ne le permet pas, l'accès direct visé à l'alinéa 1er peut être réalisé par la fourniture de fichiers de données à caractère personnel.

Les traitements des services de renseignement et de sécurité dans cette banque de données sont journalisés.

Les traitements des services de renseignement et de sécurité dans cette banque de données et leur journalisation sont protégés par des mesures de sécurité. Ces mesures sont mises à la disposition du Comité permanent R.

Si les raisons justifiant lesdits traitements doivent être enregistrées par ou en vertu de la loi, elles le sont avec la journalisation au sein de chaque service de renseignement et de sécurité concerné.

Par dérogation à l'alinéa précédent, la journalisation et les raisons justifiant le traitement peuvent être enregistrées dans la banque de données consultée, lorsque le dirigeant du service concerné estime que cet enregistrement n'est pas susceptible de porter atteinte à la protection des sources, à la protection de l'identité des agents et à la discrétion des enquêtes de renseignement. »

6° dans l'alinéa 2 ancien, devenant l'alinéa 7, la première phrase est abrogée.

A l'article 3, § 2, du même arrêté, les modifications suivantes sont apportées :

1° dans l'alinéa 1er, les mots « , sur présentation de sa carte de légitimation » sont remplacés par les mots « autorisé à y avoir accès dans la mesure où celles-ci sont utiles dans l'exercice de sa fonction ou de sa mission » ;

2° l'alinéa 3 est abrogé.

Art. 7. L'article 4 du même arrêté est abrogé.

Art. 8. Au chapitre IV du même arrêté, les modifications suivantes sont apportées :

1° la section 1re est abrogée ;

2° la section 2 est renumérotée en section 1ère ;

3° dans l'intitulé de la section 2, qui est renuméroté section 1ère, les mots « , transcriptions et traductions éventuelles des communications » sont abrogés ;

4° à l'article 7 du même arrêté, les mots « , transcriptions et traductions éventuelles des communications » sont abrogés ;

5° la section 3 est renumérotée en section 2.

Art. 9. A l'article 10, alinéa 1er du même arrêté, les modifications suivantes sont apportées :

1° les mots « alinéa 1er » sont remplacés par les mots « alinéa 5 » ;

2° le mot « immédiatement » est supprimé ;

3° les mots « aux membres » sont remplacés par les mots « au siège » ;

4° les mots « au maximum dans les vingt-quatre heures de cette autorisation » sont ajoutés à la fin de l'alinéa, après les mots « par porteur ».

Art. 10. Dans l'article 11, les alinéas 1 à 4 du même arrêté sont remplacés par ce qui suit :

« Pour l'application de l'article 43/3, alinéa 2, de la loi du 30 novembre 1998, toute décision, autorisation, avis, accord ou confirmation concernant une méthode spécifique ou exceptionnelle de recueil de données est intégralement communiqué(e) au Comité permanent R par la commission.

La commission communique également au Comité permanent R le moment où la décision lui a été notifiée.

La communication se fait sous forme numérique, sauf en cas d'impossibilité absolue ou de requête expresse du Comité permanent R. Dans ce cas, la communication peut se faire d'une autre manière, à déterminer par le Comité permanent R. ».

4° in hetzelfde lid worden de woorden "de gegevensbank" vervangen door de woorden "deze gegevensbank";

5° vijf leden worden tussen het eerste en het tweede lid ingevoegd, luidende:

"Behalve indien de opslagcapaciteit van de betrokken inlichtingen- en veiligheidsdiensten het niet toelaat, kan de rechtstreekse toegang bedoeld in het eerste lid gerealiseerd worden door het verschaffen van persoonsgegevensbestanden.

De verwerkingen van de inlichtingen- en veiligheidsdiensten in deze gegevensbank worden gelogd.

De verwerkingen van de inlichtingen- en veiligheidsdiensten en de logbestanden ervan worden beschermd door beveiligingsmaatregelen. Deze maatregelen worden ter beschikking gesteld van het Vast Comité I.

Indien de redenen die deze verwerkingen rechtvaardigen moeten opgeslagen worden door of krachtens een wet, worden ze samen met de logbestanden binnen elke betrokken inlichtingen- en veiligheidsdienst opgeslagen.

In afwijking van het voorgaande lid mogen de logbestanden en de redenen die de verwerking rechtvaardigen opgeslagen worden binnen de geraadpleegde gegevensbank, wanneer het betrokken diensthoofd van oordeel is dat deze opslag geen afbreuk kan doen aan de bescherming van de bronnen, aan de bescherming van de identiteit van de agenten en aan de discretie van de inlichtingenonderzoeken."

6° in het vroegere tweede lid, dat het zevende lid wordt, wordt de eerste zin opgeheven.

In artikel 3, § 2, van hetzelfde besluit, worden de volgende wijzigingen aangebracht:

1° in het eerste lid worden de woorden "onmiddellijk aan de agent van de inlichtingen- en veiligheidsdienst meegedeeld, op vertoon van zijn legitimatiekaart" vervangen door de woorden "onmiddellijk meegedeeld aan de agent van de inlichtingen- en veiligheidsdienst die gemachtigd is om toegang ertoe te krijgen voor zover deze nuttig is voor de uitoefening van zijn functie of opdracht";

2° het derde lid wordt opgeheven.

Art. 7. Artikel 4 van hetzelfde besluit wordt opgeheven.

Art. 8. In hoofdstuk IV van hetzelfde besluit worden de volgende wijzigingen aangebracht :

1° afdeling 1 wordt opgeheven;

2° afdeling 2 wordt vernummerd tot afdeling 1;

3° in het opschrift van afdeling 2, die vernummerd wordt tot afdeling 1, worden de woorden "en van de eventuele overschrijvingen en vertalingen van de communicaties" opgeheven;

4° in artikel 7 van hetzelfde besluit worden de woorden "en van de eventuele overschrijvingen en vertalingen van de communicaties" opgeheven;

5° afdeling 3 wordt vernummerd tot afdeling 2.

Art. 9. In artikel 10, eerste lid, van hetzelfde besluit worden de volgende wijzigingen aangebracht:

1° de woorden "eerste lid" worden vervangen door de woorden "vijfde lid";

2° het woord "onmiddellijk" wordt geschrapt;

3° de woorden "aan de leden" worden vervangen door de woorden "aan de zetel";

4° de woorden "maximaal binnen de vierentwintig uur van deze machtiging" toegevoegd aan het einde van het lid.

Art. 10. In artikel 11 worden het eerste tot het vierde lid van hetzelfde besluit vervangen als volgt:

"Voor de toepassing van artikel 43/3, tweede lid, van de wet van 30 november 1998, worden alle beslissingen, machtigingen, adviezen, akkoorden of bevestigingen met betrekking tot een specifieke of uitzonderlijke methode voor het verzamelen van gegevens integraal door de commissie ter kennis gebracht van het Vast Comité I.

De commissie geeft ook kennis aan het Vast Comité I van het moment waarop de beslissing haar werd betekend.

De kennisgeving gebeurt onder gedigitaliseerde vorm, behoudens volstrekte onmogelijkheid of ingevolge het uitdrukkelijke verzoek van het Vast Comité I. In dat geval kan de kennisgeving op een andere, door het Vast Comité I te bepalen wijze, gebeuren.".

Art. 11. Dans l'article 12 du même arrêté, les modifications suivantes sont apportées :

1° à l'alinéa 1er, les mots « des articles 18/3, § 2, alinéa 4 » sont remplacés par les mots « des articles 18/3, § 6, alinéa 3 » ;

2° à l'alinéa 2, les mots « le conseiller en sécurité de l'information et en protection de la vie privée » sont remplacés par les mots « le délégué à la protection des données ».

Art. 12. Dans le même arrêté, l'intitulé du chapitre VI est remplacé par ce qui suit :

« Chapitre VI. – De la protection des données à caractère personnel »

Art. 13. Dans le même arrêté, il est inséré un article 13/1 rédigé comme suit :

« Art. 13/1. § 1er. Un délégué à la protection des données, au sens de l'article 91 de la loi du 30 juillet 2018, est désigné au sein de chaque service de renseignement et de sécurité par le ministre compétent, sur proposition du dirigeant du service concerné.

Pour pouvoir être désigné en qualité de délégué à la protection des données au sein du service de renseignement et de sécurité concerné, le candidat doit répondre aux conditions suivantes :

1° être membre du service de renseignement et de sécurité concerné et être titulaire d'une habilitation de niveau très secret (loi 11.12.1998) ;

2° disposer d'une connaissance approfondie de la législation et d'une expérience dans le domaine de la protection des données et de la sécurité de l'information ;

3° disposer d'une connaissance approfondie des technologies de l'information en ce compris une compréhension des aspects techniques de la sécurité et des exigences spécifiques de la gestion de systèmes d'information et de services informatiques.

Un candidat peut être désigné comme délégué à la protection des données sans disposer de l'une des deux connaissances visées aux 2° et 3° de l'alinéa précédent s'il est assisté dans sa fonction par un adjoint, membre du service de renseignement et de sécurité concerné, disposant de la connaissance lui faisant défaut.

§ 2. Le délégué à la protection des données peut également remplir la fonction de conseiller en sécurité des données prévue par ou en vertu d'une loi. »

Art. 14. Dans l'article 14 du même arrêté, les modifications suivantes sont apportées :

1° à l'alinéa 1er, les mots « de l'article 13 de la loi du 8 décembre 1992, la Commission de la protection de la vie privée » sont remplacés par les mots « de la loi du 30 juillet 2018 ou de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, une autorité de protection des données » ;

2° au même alinéa, les mots « au sens de cette loi, » sont abrogés;

3° dans l'alinéa 2, troisième tiret, les mots « la Commission de la protection de la vie privée » sont remplacés par les mots « l'autorité de protection des données concernée » ;

4° dans l'alinéa 2, quatrième tiret, les mots « la Commission de la protection de la vie privée » sont remplacés par les mots « l'autorité de protection des données concernée ».

Art. 15. Dans le même arrêté, il est inséré un nouveau chapitre VII intitulé :

« CHAPITRE VII. – De la protection du personnel, des infrastructures et des biens des services de renseignement et de sécurité ».

Art. 11. In artikel 12 van hetzelfde besluit, worden de volgende wijzigingen aangebracht:

1° in het eerste lid worden de woorden "van de artikelen 18/3, § 2, vierde lid" vervangen door de woorden "van de artikelen 18/3, § 6, derde lid";

2° in het tweede lid worden de woorden "de raadgever informatieveiligheid en bescherming van de persoonlijke levenssfeer" vervangen door de woorden "de functionaris voor gegevensbescherming".

Art. 12. In hetzelfde besluit wordt het opschrift van hoofdstuk VI vervangen als volgt:

"Hoofdstuk VI. – Bescherming van persoonsgegevens"

Art. 13. In hetzelfde besluit wordt een artikel 13/1 ingevoegd, luidende:

"Art. 13/1. § 1. Binnen elke inlichtingen- en veiligheidsdienst wordt, op voordracht van het betrokken diensthoofd, een functionaris voor gegevensbescherming, in de zin van artikel 91 van de wet van 30 juli 2018, aangewezen door de bevoegde minister.

Om aangewezen te mogen worden in de hoedanigheid van functionaris voor gegevensbescherming binnen de betrokken inlichtingen- en veiligheidsdienst moet de kandidaat beantwoorden aan de volgende voorwaarden:

1° lid zijn van de betrokken inlichtingen- en veiligheidsdienst en houder zijn van een veiligheidsmachtiging van het niveau zeer geheim (wet 11.12.1998);

2° beschikken over grondige kennis van de wetgeving en over ervaring in het domein van de bescherming van de persoonsgegevens en de informatieveiligheid;

3° beschikken over grondige kennis van informatietechnologie met inbegrip van inzicht in technische beveiligingsaspecten en in de specifieke vereisten van het beheer van informatiesystemen en informatiediensten.

Een kandidaat kan aangewezen worden als functionaris voor gegevensbescherming zonder over de kennis te beschikken bedoeld in 2° en 3° van het voorgaande lid indien hij in zijn functie wordt bijgestaan door een adjunct, lid van de betrokken inlichtingen- en veiligheidsdienst, die beschikt over de kennis waaraan het hem ontbreekt.

§ 2. De functionaris voor gegevensbescherming kan ook de functie van raadsman voor de veiligheid van de gegevens vervullen zoals bepaald door of krachtens een wet.".

Art. 14. In artikel 14 van hetzelfde besluit worden de volgende wijzigingen aangebracht :

1° in het eerste lid worden de woorden "de Commissie voor de bescherming van de persoonlijke levenssfeer naar aanleiding van een verificatie op grond van artikel 13 van de wet van 8 december 1992" vervangen door de woorden "een gegevensbeschermingsautoriteit naar aanleiding van een verificatie op grond van de wet van 30 juli 2018 of de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit";

2° in het eerste lid worden de woorden "in de zin van deze wet" opgeheven.

3° in het tweede lid, derde streepje, worden de woorden "Commissie voor de bescherming van de persoonlijke levenssfeer" vervangen door de woorden "betrokken gegevensbeschermingsautoriteit";

4° in het tweede lid, vierde streepje, worden de woorden "de Commissie voor de bescherming van de persoonlijke levenssfeer" vervangen door de woorden "de betrokken gegevensbeschermingsautoriteit".

Art. 15. In hetzelfde besluit wordt een nieuw hoofdstuk VII ingevoegd, met als opschrift:

"HOOFDSTUK VII. – Bescherming van het personeel, de infrastructuur en de goederen van de inlichtingen- en veiligheidsdiensten".

Art. 16. Dans le chapitre VII, inséré par l'article 15, il est inséré un nouvel article 15 rédigé comme suit:

« Art. 15. Pour l'application de l'article 27, alinéa 4 de la loi du 30 novembre 1998, le dirigeant du service de renseignement et de sécurité concerné ou la personne qu'il désigne à cet effet, tient un registre des arrestations contenant la date, le contexte et le cas échéant, les incidents survenus. Ce registre est conservé pendant minimum dix ans après l'arrestation. »

Art. 17. Dans le même arrêté, le chapitre VII est renuméroté chapitre VIII.

Art. 18. L'article 15 du même arrêté est renuméroté article 16 et l'article 16 du même arrêté est renuméroté article 17.

CHAPITRE II. — *Modification de l'arrêté royal du 3 juillet 2016 portant exécution de l'article 21 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité*

Art. 19. Aux 2° et 3° de l'article 1er de l'arrêté royal du 3 juillet 2016 portant exécution de l'article 21 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, les mots « loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel » sont remplacés par les mots « loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ».

Art. 20. A l'article 4 du même arrêté, les mots « du conseiller en sécurité de l'information et en protection de la vie privée désigné conformément à l'article 4, § 1er, de l'arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité » sont remplacés par les mots « du délégué à la protection des données désigné conformément à l'article 91 de la loi 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ».

Art. 21. Le ministre qui a la Justice dans ses attributions et le ministre qui a la Défense dans ses attributions sont, chacun en ce qui le concerne, chargés de l'exécution du présent arrêté.

Bruxelles, le 2 octobre 2019.

PHILIPPE

Par le Roi :

Le Ministre de la Justice,
K. GEENS

Le Ministre de la Défense,
D. REYNDERS

Art. 16. In hoofdstuk VII, ingevoegd bij artikel 15, wordt een nieuw artikel 15 ingevoegd, luidend als volgt:

"Art. 15. Voor de toepassing van artikel 27, vierde lid, van de wet van 30 november 1998, houdt het diensthoofd van de betrokken inlichtingen- of veiligheidsdienst of de persoon die hij hiertoe aanstelt, een arrestatieregister bij. Het bevat de datum, de context en eventuele incidenten die zich hebben voorgedaan. Dit register wordt gedurende minstens tien jaar na de aanhouding bewaard."

Art. 17. In hetzelfde besluit wordt hoofdstuk VII vernummerd tot hoofdstuk VIII.

Art. 18. Artikel 15 van hetzelfde besluit wordt vernummerd tot artikel 16, en artikel 16 van hetzelfde besluit wordt vernummerd tot artikel 17.

HOOFDSTUK II. — *Wijziging van het koninklijk besluit van 3 juli 2016 houdende uitvoering van artikel 21 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst*

Art. 19. In artikel 1, 2° en 3° van het koninklijk besluit van 3 juli 2016 houdende uitvoering van artikel 21 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst worden de woorden "wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens" vervangen door de woorden "wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens".

Art. 20. In artikel 4 van hetzelfde besluit worden de woorden "raadgever informatieveiligheid en bescherming van de persoonlijke levenssfeer aangeduid overeenkomstig artikel 4, § 1, van het koninklijk besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten" vervangen door de woorden "functionaris voor gegevensbescherming aangeduid overeenkomstig artikel 91 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens".

Art. 21. De minister bevoegd voor Justitie en de minister bevoegd voor Defensie zijn ieder wat hun betreft, belast met de uitvoering van dit besluit.

Brussel, 2 oktober 2019.

FILIP

Van Koningswege :

De Minister van Justitie,
K. GEENS

De Minister van Defensie,
D. REYNDERS

SERVICE PUBLIC FEDERAL ECONOMIE, P.M.E., CLASSES MOYENNES ET ENERGIE

[C − 2019/42276]

17 OCTOBRE 2019. — Arrêté royal fixant pour l'année 2019 le montant de la contribution de répartition visée à l'article 14, § 8, alinéa 16, de la loi du 11 avril 2003 sur les provisions constituées pour le démantèlement des centrales nucléaires et pour la gestion des matières fissiles irradiées dans ces centrales

PHILIPPE, Roi des Belges,
A tous, présents et à venir, Salut.

Vu la loi du 11 avril 2003 sur les provisions constituées pour le démantèlement des centrales nucléaires et pour la gestion des matières fissiles irradiées dans ces centrales, l'article 14, § 8, alinéa 30, inséré par la loi du 25 décembre 2016 ;

Vu les avis (A)1923 et (A)1923*bis* de la Commission de Régulation de l'Électricité et du Gaz à la Direction Générale de l'Énergie du Service Public Fédéral Economie, P.M.E., Classes Moyennes et Énergie relatif à la marge de profitabilité de la production industrielle d'électricité par fission de combustibles nucléaires par les centrales soumises à la contribution de répartition (Doel 3, Doel 4, Tihange 2 et Tihange 3) pour l'année 2018, donnés les 27 juin 2019 et 14 août 2019 ;

FEDERALE OVERHEIDSDIENST ECONOMIE, K.M.O., MIDDENSTAND EN ENERGIE

[C − 2019/42276]

17 OKTOBER 2019. — Koninklijk besluit tot vaststelling voor het jaar 2019 van het bedrag van de repartitiebijdrage bedoeld in artikel 14, § 8, zestiende lid, van de wet van 11 april 2003 betreffende de voorzieningen aangelegd voor de ontmanteling van de kerncentrales en voor het beheer van splijtstoffen bestraald in deze kerncentrales

FILIP, Koning der Belgen,
Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Gelet op de wet van 11 april 2003 betreffende de voorzieningen aangelegd voor de ontmanteling van de kerncentrales en voor het beheer van splijtstoffen bestraald in deze kerncentrales, artikel 14, § 8, dertigste lid, ingevoegd bij de wet van 25 december 2016;

Gelet op de adviezen (A)1923 en (A)1923*bis* van de Commissie voor de Regulering van de Elektriciteit en het Gas aan de Algemene Directie Energie van de Federale Overheidsdienst Economie, K.M.O., Middenstand en Energie betreffende de winstmarge van de industriële productie van elektriciteit door splijting van kernbrandstoffen door de centrales onderworpen aan de repartitiebijdrage (Doel 3, Doel 4, Tihange 2 en Tihange 3) voor het jaar 2018, gegeven op 27 juni 2019 en 14 augustus 2019;