FEDERALE OVERHEIDSDIENST JUSTITIE EN MINISTERIE VAN LANDSVERDEDIGING

N. 2010 — 3800 [C − 2010/09868]

12 OKTOBER 2010. — Koninklijk besluit houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten

VERSLAG AAN DE KONING

Sire,

De wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten heeft de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten gewijzigd door een onderscheid te maken tussen de verschillende methoden voor het verzamelen van gegevens door de Veiligheid van de Staat en door de Algemene Dienst Inlichtingen en Veiligheid van de Krijgsmacht. Het betreft de gewone, specifieke en uitzonderlijke methoden.

De wet van 4 februari 2010 richt ook een commissie voor toezicht op die belast is met de voorafgaande controle van de uitzonderlijke methoden en met de controle tijdens het verloop van de specifieke en uitzonderlijke methoden. De controle a posteriori van de specifieke en uitzonderlijke methoden werd toegekend aan het Vast Comité I dat opgericht werd door de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse.

Deze wet, verschenen in het *Belgisch Staatsblad* op 10 maart 2010, is op 1 september 2010 in werking getreden.

Om de continuiteit van de dienst te verzekeren is het dan ook dringend dat de uitvoeringsmaatregelen van de verschillende artikelen zo snel mogelijk in werking treden.

Bij ontstentenis zal de wet van 4 februari 2010 niet ten volle in uitvoering kunnen worden gebracht.

Bepaalde methoden, zoals observaties en schaduwingen die, naast het verzamelen van louter administratieve gegevens, op heden deel uitmaken van de essentiële middelen voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten, kunnen niet meer uitgevoerd worden in hangende zaken zonder voorafgaandelijke notificatie aan de commissie. Dit zal leiden tot een aanzienlijk verlies van operationele onderzoekscapaciteit van de inlichtingen- en veiligheidsdiensten, namelijk in het kader van terrorismebestrijding, met inbegrip van radicalisme.

De wet van 4 februari 2010 neemt dus in de wet van 30 november 1998 talloze artikelen op en vertrouwt aan de Koning de zorg toe om de nadere regels voor uitvoering van sommige artikelen te bepalen.

In het kader van dit besluit gaat het om de artikelen 13/1, § 1, 14, vierde lid, 18/3, § 2, 18/10, § 1, derde lid, § 4, eerste lid en § 6, vierde lid, 18/13, tweede lid, 18/17, § 7, 18/18, 43/3, 43/4 en 43/6.

In het kader van de uitoefening van zijn opdrachten kan een agent van de inlichtingen- en veiligheidsdiensten zo, in afwijking van artikel 231 van het Strafwetboek, omwille van veiligheidsredenen verbonden aan de bescherming van zijn persoon en voor de behoeften eigen aan de uitoefening van de opdracht, een naam gebruiken die hem niet toebehoort, volgens de door de Koning te bepalen nadere regels : art. 13/1, § 1, van de wet van 30 november 1998;

Met inachtneming van de geldende wetgeving kunnen de inlichtingen- en veiligheidsdiensten, overeenkomstig de door de Koning vastgelegde algemene nadere regels, toegang krijgen tot de gegevensbanken van de openbare sector die nuttig zijn voor de uitoefening van hun opdrachten : art. 14, vierde lid, van de wet van 30 november 1998;

De gegevens verkregen door middel van specifieke en uitzonderlijke methoden in omstandigheden die de vigerende wettelijke bepalingen niet naleven, worden onder controle van de commissie voor toezicht bewaard, overeenkomstig de door de Koning bepaalde nadere regels en termijnen, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer : art. 18/3, § 2 en 18/10, § 6, vierde lid, van dezelfde wet;

Wanneer het Vast Comité I tijdens zijn controle a posteriori vaststelt dat gegevens onwettig verzameld werden, beveelt het hun vernietiging, volgens de door de Koning bepaalde nadere regels, na advies van de Commissie voor bescherming van de persoonlijke levenssfeer en van het Vast Comité I : art. 43/6, § 1 van dezelfde wet;

Het diensthoofd van de betrokken dienst licht de commissie in over de uitvoering van de uitzonderlijke methode, overeenkomstig de door de Koning bepaalde nadere regels en termijnen : art. 18/10, § 1, derde lid, van dezelfde wet;

SERVICE PUBLIC FEDERAL JUSTICE ET MINISTERE DE LA DEFENSE

F. 2010 — 3800 [C − 2010/09868]

12 OCTOBRE 2010. — Arrêté royal portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

RAPPORT AU ROI

Sire,

La loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité a modifié la loi du 30 novembre 1998 organique des services de renseignement et de sécurité en distinguant les différentes catégories de méthodes de recueil des données effectuées par la Sûreté de l'Etat et le Service général du renseignement et de la sécurité des Forces armées. Il s'agit des méthodes ordinaires, spécifiques et exceptionnelles.

La loi du 4 février 2010 crée également une commission de surveillance chargée du contrôle a priori des méthodes exceptionnelles et du contrôle pendant le déroulement des méthodes spécifiques et exceptionnelles. Le contrôle a posteriori des méthodes spécifiques et exceptionnelles a été attribué au Comité permanent R, créé par la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace.

Cette loi, parue au *Moniteur belge* le 10 mars 2010, est entrée en vigueur le 1er septembre 2010.

Il est donc urgent pour assurer la continuité des services que les mesures d'exécution des différents articles de la loi entrent en vigueur le plus rapidement possible.

A défaut, la loi du 4 février 2010 ne pourra être mise en œuvre entièrement.

Certaines méthodes, telles que les observations et filatures, qui, outre le recueil de données purement administratives, font partie, à l'heure actuelle, des moyens essentiels de recueil des données par les services de renseignement et de sécurité, ne pourront plus être exécutées, dans des affaires en cours, sans la notification préalable à la commission. Ce qui entraînera une perte importante de la capacité opérationnelle d'investigation des services de renseignement et de sécurité, notamment dans le cadre de la lutte contre le terrorisme, y compris le radicalisme.

La loi du 4 février 2010 insère donc, dans la loi du 30 novembre 1998, de nombreux articles et confie au Roi le soin de déterminer les modalités d'exécution de certains d'entre eux.

Il s'agit dans le cadre du présent arrêté des articles 13/1, § 1er, 14, alinéa 4, 18/3, § 2, 18/10, § 1er, alinéa 3, § 4, alinéa 1er et § 6, alinéa 4, 18/13, alinéa 2, 18/17, § 7, 18/18, 43/3, 43/4 et 43/6.

Ainsi, dans le cadre de l'exécution de ses missions, par dérogation à l'article 231 du Code pénal, un agent des services de renseignement et de sécurité peut, pour des raisons de sécurité liées à la protection de sa personne et pour les besoins inhérents à l'exercice d'une mission, utiliser un nom qui ne lui appartient pas, selon les modalités à fixer par le Roi : art. 13/1, § 1er, de la loi du 30 novembre 1998;

Dans le respect de la législation en vigueur, les services de renseignement et de sécurité peuvent, selon les modalités générales fixées par le Roi, avoir accès aux banques de données du secteur public utiles à l'exécution de leurs missions : art. 14, alinéa 4, de la loi du 30 novembre 1998;

Les données recueillies, au moyen des méthodes spécifiques et exceptionnelles, dans des conditions qui ne respectent pas les dispositions légales en vigueur, sont conservées, sous le contrôle de la commission de surveillance, selon les modalités et délais fixés par le Roi, après avis de la Commission de la protection de la vie privée : art. 18/3, § 2 et 18/10, § 6, alinéa 4, de la même loi;

Si, lors de son contrôle a posteriori, le Comité permanent R constate que des données ont été recueillies illégalement, il ordonne leur destruction, selon les modalités à fixer par le Roi, après avis de la Commission de la protection de la vie privée et du Comité permanent R : art. 43/6, § 1er, de la même loi;

Le dirigeant du service concerné informe la commission de surveillance de l'exécution de la méthode exceptionnelle, selon les modalités et délais déterminés par le Roi : art. 18/10, § 1er, alinéa 3, de la même loi;

In geval van uiterste hoogdringendheid kan het diensthoofd, nadat hij het eensluidend advies van de voorzitter van de commissie heeft verkregen, de uitzonderlijke methode voor het verzamelen van gegevens schriftelijk machtigen voor ten hoogste achtenveertig uur. Deze machtiging vermeldt de redenen die de uiterste hoogdringendheid wettigen en wordt onmiddellijk ter kennis gebracht van alle leden van de commissie volgens de door de Koning te bepalen nadere regels : art. 18/10, § 4, eerste lid, van dezelfde wet;

In het kader van de uitzonderlijke methode die erin bestaat om rechtspersonen op te richten en in te zetten ter ondersteuning van de operationele activiteiten, kunnen agenten ingezet worden onder de dekmantel van een fictieve identiteit of hoedanigheid, conform de door de Koning bepaalde nadere regels : art. 18/13, tweede lid, van dezelfde wet;

Artikel 18/17 betreft de uitzonderlijke methode die erin bestaat om communicaties af te luisteren, er kennis van te nemen en ze te registreren. Deze bepaling voorziet onder andere dat de opnamen, alsook de eventuele overschrijving en de eventuele vertaling, vernietigd worden volgens de door de Koning te bepalen nadere regels : art. 18/17, § 7, van dezelfde wet;

De Koning legt de tarieven vast voor de medewerking van fysieke personen en rechtspersonen aan een uitzonderlijke methode, waarbij Hij rekening houdt met de werkelijke kostprijs van deze medewerking : art. 18/18 van dezelfde wet;

De lijsten van de specifieke methoden worden door de bevoegde overheid onverwijld ter kennis gebracht aan het Vast Comité I, overeenkomstig de door de Koning te bepalen modaliteiten : art. 43/3 van dezelfde wet;

Tenslotte handelt het Vast Comité I in het kader van zijn toezicht op de wettigheid, met name op verzoek van de Commissie voor de bescherming van de persoonlijke levenssfeer, volgens de nadere regels door de Koning bepaald, bij een besluit vastgesteld na overleg in de Ministerraad, na advies van dezelfde Commissie en van het Vast Comité I : art. 43/4 van dezelfde wet.

De bepalingen betreffende elektronische communicaties (art. 18/7, 18/8 en 18/17) en het secretariaat van de commissie (art. 43/1) worden uitgevoerd door twee andere, verschillende besluiten rekening houdende met het specifiek karakter van de behandelde materies.

Bij het opstellen van dit besluit werd rekening gehouden met de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, gewijzigd bij wet van 3 mei 2005, met het koninklijk besluit van 24 maart 2000 tot uitvoering van deze wet en met de richtlijnen van het Ministerieel Comité voor inlichting en veiligheid ter uitvoering ervan.

Toelichting van de artikelen

Hoofdstuk II. — *Uitoefening van inlichtingen- en veiligheidsopdrachten*

Gebruik van een valse naam

Artikel 2

Artikel 2 bepaalt de regels voor het gebruik van een valse naam. Het voorziet ook dat het diensthoofd, of de persoon die hij hiertoe aanstelt, lijsten bijhoudt met de valse namen die door de agenten van de diensten gebruikt worden. Er dient immers bepaald te kunnen worden met welke agent een valse naam overeenstemt. Zo kan zowel de bescherming van de operationele behoeften van de dienst als de traceerbaarheid van het gebruik van de valse naam in geval van een eventueel incident verzekerd worden. Daarom is ook voorzien dat een agent die een valse naam gebruikt, een logboek bijhoudt, waarin hij de data en de context van het gebruik van de valse naam schrijft en waarin hij ook de incidenten vermeldt die plaatsgevonden zouden hebben. Dit logboek maakt het voorwerp uit van een controle door het diensthoofd of de persoon die hiertoe aangesteld wordt, en kan een nuttig document zijn voor het Vast Comité I bij de uitvoering van zijn controle.

In tegenstelling tot hetgeen de Commissie voor de bescherming van de persoonlijke levenssfeer stelt in haar samenvatting van artikel 2 van het ontwerp, is het evenwel niet het diensthoofd dat het logboek bijhoudt, maar de agent die de valse naam gebruikt. Deze opmerking geldt eveneens voor artikel 6 van dit besluit dat handelt over de valse identiteit en hoedanigheid.

Omwille van duidelijke redenen van vertrouwelijkheid worden de documenten betreffende de valse namen die door de agenten van de inlichtingen- en veiligheidsdiensten gebruikt worden, geclassificeerd overeenkomstig de wet van 11 december 1998.

Hoofdstuk III. — *Gewone methoden voor het verzamelen van gegevens*

Toegang tot de gegevensbanken van de openbare sector

Artikel 3

De inlichtingen- en veiligheidsdiensten kunnen toegang hebben tot de gegevensbanken van de openbare diensten, met inachtneming van de geldende wetgeving die hierop van toepassing is. Binnen dit kader

Dans les cas d'extrême urgence, le dirigeant du service peut autoriser par écrit la méthode exceptionnelle de recueil de données pour une durée qui ne peut excéder quarante-huit heures, après avoir obtenu au préalable, l'avis conforme du président de la commission de surveillance. Cette autorisation indique les motifs qui justifient l'extrême urgence et est immédiatement communiquée à l'ensemble des membres de la commission selon les modalités à fixer par le Roi : art. 18/10, § 4, alinéa 1er, de la même loi;

Dans le cadre de la méthode exceptionnelle consistant à créer ou recourir à des personnes morales à l'appui des activités opérationnelles, les agents du service peuvent être couverts par une identité ou une qualité fictive, conformément aux modalités fixées par le Roi : art. 18/13, alinéa 2, de la même loi;

L'article 18/17 concerne la méthode exceptionnelle qui consiste à écouter les communications, à en prendre connaissance et à les enregistrer. Cette disposition prévoit, entre autres, que les enregistrements, ainsi que la transcription éventuelle et leur traduction éventuelle sont détruits, selon les modalités à fixer par le Roi : art. 18/17, § 7, de la même loi;

Les tarifs rétribuant les personnes physiques et les personnes morales, qui apportent leur collaboration à une méthode exceptionnelle, sont fixés par le Roi, en tenant compte du coût réel de cette collaboration : art. 18/18 de la même loi;

Les listes des méthodes spécifiques sont portées sans délai à la connaissance du Comité permanent R par l'autorité compétente, suivant les modalités à fixer par le Roi : art. 43/3 de la même loi;

Enfin, dans le cadre de son contrôle de légalité, le Comité permanent R agit, notamment, à la demande de la Commission de la protection de la vie privée suivant les modalités déterminées par le Roi, par arrêté délibéré en Conseil des Ministres, après avis de ladite Commission et du Comité permanent R : art. 43/4 de la même loi.

En ce qui concerne les dispositions relatives aux télécommunications (art. 18/7, 18/8 et 18/17) et celles relatives au secrétariat de la commission (art. 43/1), elles sont exécutées par deux autres arrêtés distincts, compte tenu de la spécificité des matières traitées.

Lors de la rédaction du présent arrêté, il a été tenu compte de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, modifiée par la loi du 3 mai 2005, de l'arrêté royal du 24 mars 2000 portant exécution de cette loi et des directives du Comité ministériel du renseignement et de la sécurité prises en exécution de celui-ci.

Commentaire des articles

Chapitre II. — *De l'exercice des missions de renseignement et de sécurité*

Utilisation d'un faux nom

Article 2

L'article 2 détermine les modalités d'utilisation d'un faux nom. Il prévoit ainsi que le dirigeant du service, ou la personne qu'il désigne à cet effet, tient des listes des faux noms utilisés par les agents des services. Il convient, en effet, de pouvoir déterminer à quel agent correspond tel faux nom et ce, pour assurer tant la protection des nécessités opérationnelles du service que la traçabilité de l'utilisation du faux nom en cas d'incident éventuel. C'est la raison pour laquelle il est également prévu que, lorsqu'un agent utilise un faux nom, il tient un journal de bord où il inscrit les dates et le contexte de l'utilisation du faux nom et qu'il y mentionne également les incidents qui seraient survenus. Ce journal de bord fait l'objet d'un contrôle par le dirigeant du service ou la personne qu'il désigne à cet effet, et peut constituer un document utile, pour le Comité permanent R, à l'exercice de son contrôle.

Toutefois, contrairement à ce qu'affirme la Commission de la protection de la vie privée dans son résumé de l'article 2 du projet, ce n'est pas le dirigeant du service qui tient le journal de bord mais l'agent qui utilise le faux nom. La remarque vaut également pour l'article 6 du présent arrêté qui concerne les identité et qualité fictives.

Pour des raisons évidentes de confidentialité, les documents relatifs aux faux noms utilisés par les agents des services de renseignement et de sécurité sont classifiés conformément à la loi du 11 décembre 1998.

Chapitre III. — *Des méthodes ordinaires de recueil des données*

Accès aux banques de données du secteur public

Article 3

Les services de renseignement et de sécurité peuvent avoir accès aux banques de données des services publics, dans le respect de la législation en vigueur qui leur est applicable. Il importe, dans ce cadre,

is het belangrijk dat de eisen van directe toegang (te weten de toegang online) tot de gegevensbanken identiek zijn, met name wat de controle van deze toegangen betreft. Wanneer deze gegevensbanken persoonsgegevens bevatten, is voorzien dat een nominatieve lijst van de personen die gemachtigd zijn om toegang te hebben tot de gegevensbank, ter beschikking van de Commissie voor de bescherming van de persoonlijke levenssfeer wordt gehouden.

De principes vermeld in artikel 3, § 1, staan reeds in het koninklijk besluit van 10 augustus 2001 waarbij aan de Veiligheid van de Staat toegang wordt verleend tot het Rijksregister van de natuurlijke personen (*Belgisch Staatsblad* 7 september 2001) en in het koninklijk besluit van 28 februari 2002 betreffende de mededeling van informatie door gemeenten aan de Veiligheid van de Staat door toedoen van het Rijksregister van de natuurlijke personen. (*Belgisch Staatsblad* 29 maart 2002). Hetzelfde geldt in het koninklijk besluit van 8 juli 1999 waarbij de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht toegang wordt verleend tot het Rijksregister van de natuurlijke personen (*Belgisch Staatsblad* 7 augustus 1999).

Deze besluiten voorzien een registratie van de consulterende agenten gedurende een periode van 6 maanden.

Wanneer een rechtstreekse toegang niet mogelijk is, bijvoorbeeld omwille van wettelijke redenen, wordt de informatie ter plaatse aan de agent van de inlichtingen- en veiligheidsdienst gegeven, op vertoon van zijn legitimatiekaart.

De principes vermeld in artikel 3, § 2, zijn gebaseerd op het koninklijk besluit van 6 oktober 2000 betreffende de mededeling door de gemeenten aan de Veiligheid van de Staat van inlichtingen die zich bevinden in bevolkings- en vreemdelingenregisters (*Belgisch Staatsblad* 11 november 2000) evenals op het koninklijk besluit van 8 juli 1999 betreffende de mededeling door de gemeenten van informatie, opgenomen in de bevolkingsregisters en het vreemdelingregister, aan de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht (*Belgisch Staatsblad* 7 augustus 1999).

Ingevolge het advies 24/2010 van de Commissie voor de bescherming van de persoonlijke levenssfeer wordt de identiteit van de consulterende agenten geregistreerd voor een periode van tien jaar – in de plaats van de aanvankelijk voorziene twaalf maanden – in een controlesysteem binnen de betrokken inlichtingen- en veiligheidsdienst.

In dit verband constateert de Raad van State dat dit controlesysteem verschilt van dat van bijzondere koninklijke besluiten, bijvoorbeeld met betrekking tot het rijksregister. Het is dan ook aan te bevelen deze in het verleden aangenomen bijzondere koninklijke besluiten aan te passen ten aanzien van artikel 3 van dit besluit.

De Commissie voor de bescherming van de persoonlijke levenssfeer beveelt eveneens aan dat, zoals voorzien is voor de directe toegang, de aanvragen en raadplegingen die gebeuren op vertoon van de legitimatiekaart van de agenten van de inlichtingen- en veiligheidsdiensten, door de verantwoordelijke van de gegevensbank geregistreerd worden in een logboek.

Behalve dat deze procedure in deze hypothese buitensporig zwaar is, blijft er steeds een geschreven spoor van de door de agenten van de inlichtingen- en veiligheidsdiensten op basis van hun legitimatiekaart gevraagde raadplegingen, en worden zij geregistreerd in de gegevensbank van deze diensten in de mate waarin zij de onderzoeken voeden en bijgevolg noodzakelijkerwijze hun weerslag vinden in de daaruit voortvloeiende rapporten. De traceerbaarheid is dus gewaarborgd en de meerwaarde van deze aanbeveling is bijgevolg niet merkbaar gezien er de facto in praktijk reeds aan voldaan is.

Wat de toegang tot de gegevensbanken van de openbare sector in het algemeen betreft, doet de Commissie voor de bescherming van de persoonlijke levenssfeer opmerken dat artikel 14, vierde lid, van de organieke wet stilzwijgend voorbij gaat aan het feit dat de toegang tot deze gegevensbanken ook op geheime wijze kan gebeuren. Als een dergelijke geheime raadpleging uitgevoerd zou zijn die, volgens de Commissie voor de bescherming van de persoonlijke levenssfeer, een degelijke motivering en het advies van de bestuurlijke commissie zou vereisen, is zij van mening dat het gepast zou zijn om de beheerder van de gegevensbank hiervan op de hoogte te brengen via een kennisgeving die tot enkele personen beperkt is om de geheime aard van het inlichtingenwerk niet in gevaar te brengen.

Deze opmerking doet vragen rijzen. In de eerste plaats dient eraan herinnerd te worden dat artikel 14 van de organieke wet zich op het niveau van de gewone methoden van de inlichtingendiensten situeert. Zich op geheime wijze toegang verschaffen tot een gegevensbank zou neerkomen op indringen in een informaticasysteem, wat een uitzonderlijke methode vormt waarvoor het voorafgaand conform advies van de bestuurlijke commissie vereist is.

que les exigences d'accès direct (c'est-à-dire l'accès on-line) aux banques de données soient identiques, notamment quant au contrôle de ces accès. Lorsque les banques de données contiennent des données à caractère personnel, il est prévu qu'une liste nominative des personnes habilitées à accéder à la banque de données est tenue à la disposition de la Commission de la protection de la vie privée.

Les principes repris à l'article 3, § 1er figurent déjà dans l'arrêté royal du 10 août 2001 autorisant l'accès de la Sûreté de l'Etat au Registre national des personnes physiques (*Moniteur belge* 7 septembre 2001) et dans 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. (*Moniteur belge* 29 mars 2002). Il en est de même dans l'arrêté royal du 8 juillet 1999 autorisant l'accès du Service général du Renseignement et de Sécurité des Forces armées au Registre national des personnes physiques. (*Moniteur belge* 7 août 1999).

Ces arrêtés prévoient un enregistrement de l'identité des agents consultants pendant une période de 6 mois.

Lorsqu'un accès direct n'est pas possible, par exemple, pour des raisons légales, l'agent des services de renseignement et de sécurité qui se rend sur place, reçoit l'information sur présentation de sa carte de légitimation.

Les principes repris à l'article 3, § 2 s'inspirent de l'arrêté royal du 6 octobre 2000 relatif à la communication par les communes, à la Sûreté de l'Etat, d'informations contenues dans les registres de la population et des étrangers (*Moniteur belge* 11 novembre 2000), ainsi que de l'arrêté royal du 8 juillet 1999 relatif à la communication par les communes au Service Général de Renseignement et de la Sécurité des Forces armées, d'informations contenues dans les registres de la population et des étrangers (*Moniteur belge* 7 août 1999).

Suite à l'avis 24/2010 de la Commission de la protection de la vie privée, l'identité des agents consultants est enregistrée, pendant dix ans - au lieu des douze mois initialement prévus - dans un système de contrôle au sein du service de renseignement et de sécurité concerné.

A cet égard, le Conseil d'Etat constate que ce système de contrôle diffère de celui des arrêtés royaux particuliers relatifs au registre national par exemple. Il conviendra donc d'adapter ces arrêtés royaux particuliers pris dans le passé au regard de l'article 3 du présent arrêté.

La Commission de la protection de la vie privée recommande également qu'à l'instar de ce qui est prévu pour l'accès direct, une journalisation des demandes et des consultations effectuées sur présentation de la carte de légitimation des agents des services de renseignement et de sécurité fasse l'objet d'un enregistrement par le gestionnaire de la base de données.

Outre que cette procédure apparait d'une lourdeur excessive dans cette hypothèse, les consultations demandées par les agents des services de renseignement et de sécurité, sur la base de leur carte de légitimation, font toujours l'objet d'une trace écrite et d'un enregistrement dans la base de données de ces services, dans la mesure où elles servent à alimenter des enquêtes et se retrouvent donc nécessairement dans les rapports qui en découlent. La traçabilité en est assurée et on n'aperçoit dès lors pas la valeur ajoutée de cette recommandation étant donné que, de facto, elle est déjà rencontrée par la pratique.

En ce qui concerne l'accès aux banques de données du secteur public en général, la Commission de la protection de la vie privée relève que l'article 14, alinéa 4 de la loi organique passe sous silence le fait de savoir si l'accès à ces banques de données peut également se faire de manière secrète. Si une telle consultation secrète était effectuée, laquelle, selon la Commission de la protection de la vie privée, nécessiterait une solide motivation et l'avis de la commission administrative, elle estime qu'il serait opportun d'en informer le gestionnaire de la banque de données, par une notification limitée à quelques personnes, afin de ne pas compromettre le caractère secret du travail de renseignement.

Cette remarque pose question. Au premier chef, il convient de rappeler que larticle 14 de la loi organique se situe au niveau des méthodes ordinaires des services de renseignement. Or, s'introduire de manière secrète dans une banque de données reviendrait à pratiquer une intrusion dans un système informatique, ce qui constitue une méthode exceptionnelle nécessitant l'avis conforme préalable de la commission administrative.

Aangezien het bovendien om de rechtstreekse toegang (d.w.z. online) tot een gegevensbank gaat, kunnen we niet spreken van een geheime raadpleging vermits de toegang door de beheerder van de gegevensbank toegestaan wordt. Het spreekt voor zich dat de leden van de inlichtingen- en veiligheidsdiensten, die met naam aangesteld zijn om toegang te hebben tot de gegevensbank, de beheerder hiervan niet bij iedere raadpleging op de hoogte moeten brengen. Het is net daarom dat de identiteit van de consulterende agenten geregistreerd wordt.

Als de toegang niet rechtstreeks is, wordt de vraag vanzelf opgelost, aangezien men noodzakelijk via een tussenpersoon moet handelen om de gewenste informatie te bekomen.

Bovendien is, in navolging van hetgeen nu voorzien is in het koninklijk besluit van 28 februari 2002 betreffende de mededeling van informatie door gemeenten aan de Veiligheid van de Staat door toedoen van het Rijksregister van de natuurlijke personen, in artikel 4 voorzien dat een raadsman voor de veiligheid van de gegevens aangesteld wordt in elke inlichtingen- en veiligheidsdienst, dat hij toeziet op de naleving van de wet bij iedere vraag om gegevens en dat hij alle nuttige maatregelen neemt teneinde de veiligheid van de geregistreerde informatie te verzekeren.

Deze regel die alleen maar voorzien was in het voornoemd koninklijk besluit van 28 februari 2002 voor de Veiligheid van de Staat, wordt nu als algemene regel ingesteld en is van toepassing op elke inlichtingen- en veiligheidsdienst.

Artikel 4

In bovenvermeld advies merkt de Commissie voor de bescherming van de persoonlijke levenssfeer niettemin op dat een andere terminologie, namelijk « raadsman voor de veiligheid van de gegevens » gebruikt werd in vergelijking met de bestaande terminologie van artikel 17*bis* van de WVP (aangestelde voor de gegevensbescherming) of met artikel 10 van de wet van 8 augustus 1983 tot regeling van een Rijksregister voor de natuurlijke personen (consulent inzake informatieveiligheid). Het risico hiervan is dat dit eventueel zou kunnen leiden tot een afwijkende interpretatie en de Commissie raadt dus aan om naar één van beiden te verwijzen.

Artikel 4 voorziet dus nu de aanstelling binnen iedere inlichtingen- en veiligheidsdienst van een « raadgever informatieveiligheid en bescherming van de persoonlijke levenssfeer, die onder andere de functie van aangestelde voor de gegevensbescherming uitvoert » in de plaats van een raadsman voor de veiligheid van de gegevens, wat aanvankelijk in deze tekst voorzien was.

Er wordt dus gekozen voor een terminologie die gebaseerd is op de bovenvermelde wet van 8 augustus 1983. De term « raadgever informatieveiligheid en bescherming van de persoonlijke levenssfeer » wordt gebruikt in de plaats van de term « consulent inzake de informatieveiligheid en bescherming van de persoonlijke levenssfeer » van artikel 10 van deze wet. Het woord « consulent » verwijst immers meer naar een expertise extern aan de dienst, terwijl enkel een lid van de dienst aangesteld zal kunnen worden om deze functie uit te oefenen wegens het geheim karakter van het werk van de inlichtingendiensten en het delicaat aspect van zijn gegevensbank.

Overeenkomstig de wens van de Commissie zal deze « raadgever informatieveiligheid » ook de functie van « aangestelde voor de gegevensbescherming », bedoeld in artikel 17*bis* van de WVP, op zich nemen.

Anderzijds benadrukt de Commissie het belang van de onafhankelijke positie van de « raadgever informatieveiligheid » en preciseert ze dat hij enkel aan het betrokken diensthoofd rekenschap moet afleggen en verslag uitbrengen.

Daarentegen is het niet duidelijk waarom hij zou moeten verslag uitbrengen bij de commissie terwijl deze enkel bevoegd is voor de specifieke en uitzonderlijke methoden. Zoals hierboven reeds in herinnering gebracht is de toegang tot gegevensbanken een gewone methode. Daarenboven kan de commissie, in voorkomend geval, de leden van de dienst horen, met inbegrip de « raadgever informatieveiligheid ». Hetzelfde geldt voor het Comité I op grond van de artikelen 43/5, §§ 2 en 4 van de wet van 30 november 1998.

De tekst van artikel 4, § 1, tweede lid, wordt aangepast aan het advies van de commissie dat bovendien preciseert dat deze raadgever op onafhankelijke wijze handelt in het kader van zijn functie :

— het waarborgen van de naleving van de wet bij iedere vraag om gegevens;

— het nemen van alle nuttige maatregelen teneinde de veiligheid van de geregistreerde informatie te verzekeren;

— het verstrekken van geschikte adviezen aan het diensthoofd;

— het uitvoeren van andere opdrachten die hem door het diensthoofd toevertrouwd zijn.

En outre, s'agissant de l'accès direct (c'est-à-dire on-line) à une banque de données, on ne peut pas parler d'une consultation secrète, puisque l'accès est autorisé par le gestionnaire de la banque de données. Il est clair que les membres des services de renseignement et de sécurité, qui sont nommément désignés pour avoir accès à la banque de données, ne sont pas tenus d'avertir le gestionnaire de celle-ci, lors de chaque consultation. C'est pour cette raison, précisément, qu'il y a un enregistrement de l'identité des agents consultants.

Si l'accès n'est pas direct, la question est réglée par elle-même, puisqu'il faut nécessairement passer par un intermédiaire pour obtenir l'information souhaitée.

Par ailleurs, à l'instar de ce qui est actuellement prévu dans 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, il est prévu, à l'article 4, qu'un conseiller à la sécurité des données est désigné au sein de chaque service de renseignement et de sécurité et qu'il veille 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.

Cette règle qui n'était prévue que dans l'arrêté royal précité du 28 février 2002, pour la Sûreté de l'Etat, est érigée en règle générale applicable à chaque service de renseignement et de sécurité.

Article 4

Cependant, dans son avis précité, la Commission de la protection de la vie privée relève qu'une terminologie différente, à savoir « conseiller à la sécurité des données », était employée par rapport aux terminologies existantes de l'article 17*bis* de la LVP (préposé à la protection des données) ou de l'article 10 de la loi du 8 août 1983 organisant un Registre national des personnes physiques (consultant en sécurité de l'information), au risque de créer éventuellement une divergence d'interprétation et recommande dès lors de se référer à l'une ou à l'autre.

L'article 4 prévoit donc, maintenant, la désignation, au sein de chaque service de renseignement et de sécurité, d'un « conseiller en sécurité de l'information et en protection de la vie privée, qui remplit, entre autres, la fonction de préposé à la protection des données », au lieu d'un conseiller à la sécurité des données initialement prévu par ce texte.

Il est donc opté pour une terminologie inspirée de la loi du 8 août 1983 précitée. En effet, les termes « conseiller en sécurité de l'information et en protection de la vie privée » sont utilisés en lieu et place des termes « consultant en sécurité de l'information et en protection de la vie privée » de l'article 10 de cette loi. Car le vocable « consultant » fait davantage référence à une expertise externe au service, alors qu'en raison du caractère secret du travail des services de renseignement et de l'aspect délicat de sa banque de données, seul un membre du service pourra être désigné pour exercer cette fonction.

Conformément au vœu de la Commission, ce « conseiller en sécurité de l'information » remplira aussi la fonction de « préposé à la protection des données » visé à l'article 17*bis* de la LVP.

D'autre part, la Commission insiste sur l'importance de la position indépendante du « conseiller en sécurité de l'information » et précise qu'il ne doit rendre des comptes et faire rapport qu'au dirigeant du service concerné.

Par contre, on n'aperçoit pas pourquoi il devrait faire rapport à la commission, alors que celle-ci n'est compétente que pour les méthodes spécifiques et exceptionnelles. Comme rappelé ci-dessus, l'accès aux banques de données constitue une méthode ordinaire. Qui plus est, la commission peut entendre les membres du service, le cas échéant, en ce compris le « conseiller en sécurité de l'information ». Il en va de même pour le Comité R, en vertu des articles 43/5, §§ 2 et 4 de la loi du 30 novembre 1998.

Le texte de l'article 4, § 1er, alinéa 2, se conforme à l'avis de la Commission qui précise, en outre, que ce conseiller agit de manière indépendante dans le cadre de sa fonction :

— de veiller au respect de la loi lors de toute demande de données;

— de prendre toutes mesures utiles afin d'assurer la sécurité des informations enregistrées;

— de fournir des avis qualifiés au dirigeant du service;

— d'exécuter d'autres missions qui lui sont confiées par le dirigeant du service.

De opdrachten van de raadgever informatieveiligheid werden aangevuld teneinde ze beter te preciseren. Hierbij diende artikel 9 van de wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealth-platform als basis.

Toch is de Commissie voor de bescherming van de persoonlijke levenssfeer van mening dat de raadgever informatieveiligheid een statutaire bescherming zou moeten genieten, zoals die van de leden van het controleorgaan van de politie-informatie (cfr. artikel 44/7, laatste lid, van de wet op het politieambt), teneinde zijn functie in alle onafhankelijkheid te kunnen vervullen.

Er dient echter vastgesteld te worden dat artikel 14, vierde lid, van de organieke wet geen bevoegdheid voor de Koning omvat om het statuut van de raadgever informatieveiligheid te regelen, maar enkel om de algemene bepalingen inzake toegang tot de gegevensbanken van de openbare sector die nuttig zijn voor de uitoefening van hun opdrachten, door de effectieve aanwezigheid van een dergelijke raadsman binnen de inlichtingen- en veiligheidsdiensten, te regelen.

Merk overigens op dat het statuut van de personen die een gelijkaardige opdracht moeten uitoefenen krachtens andere wetgevingen, over het algemeen nog niet geregeld is, te beginnen met artikel 17*bis* van de wet van 8 december 1992 dat als wettelijke referentiebasis had kunnen fungeren.

Paragraaf 2 voorziet dat voor de Veiligheid van de Staat de thans aangestelde raadsman voor de veiligheid van de gegevens de functie van raadgever informatieveiligheid en bescherming van de persoonlijke levenssfeer vervult, die onder andere de functie van aangestelde voor de gegevensbescherming, bedoeld in artikel 4, uitoefent.

De huidige raadsman voor de veiligheid van de gegevens werd door de minister van Justitie aangesteld overeenkomstig artikel 6 van het koninklijk besluit van 28 februari 2002 betreffende de mededeling van informatie door gemeenten aan de Veiligheid van de Staat door toedoen van het Rijksregister van natuurlijke personen. Zo wordt beantwoord aan het advies nr. 5/2000 van 13 maart 2000 van de Commissie voor de bescherming van de persoonlijke levenssfeer en aan het advies van de Raad van State dat over dit besluit gegeven werd.

Zijn missie zal dus uitgebreid worden tot de gegevensbanken van de publieke sector waartoe de inlichtingen- en veiligheidsdiensten toegang zullen hebben in toepassing van artikel 14, vierde lid, van de wet van 30 november 1998.

Artikel 5

Artikel 5 voorziet dat de inlichtingen- en veiligheidsdiensten kosteloos toegang hebben tot de gegevensbanken van de openbare sector. Deze vrijstelling wordt gerechtvaardigd door het feit dat de inlichtingendiensten overheidsdiensten zijn die de opdracht hebben om de fundamentele belangen van de Staat te beschermen. Het zou dus niet logisch zijn dat de Staat de Staat zou betalen voor diensten die door de Staat geleverd worden met het oog op de bescherming ervan.

Hoofdstuk IV. — *Specifieke methoden en uitzonderlijke methoden voor het verzamelen van gegevens*

Afdeling 1. — Fictieve identiteiten en hoedanigheden

Artikel 6

Hoewel het gebruik van een valse naam een gewone methode is, is het gebruik van een valse identiteit of hoedanigheid verbonden met de oprichting of het gebruik van rechtspersonen, een uitzonderlijke methode, zoals beschreven in artikel 18/13 van de wet van 30 november 1998, ingevoegd door de wet van 4 februari 2010. De fictieve identiteit of hoedanigheid dekt de agent van de inlichtingendienst belast met het op gerichte wijze verzamelen van gegevens omtrent gebeurtenissen, voorwerpen, groeperingen en natuurlijke personen of rechtspersonen die een belang vertonen voor de uitoefening van de opdrachten. Laten we preciseren dat de uitzonderlijke methoden enkel aangewend kunnen worden in het kader van bedreigingen, zoals bedoeld in artikel 18/9, § 1, nieuw, van de wet van 30 november 1998.

De rechtspersoon opgericht ter ondersteuning van operationele activiteiten kan een langere levensduur hebben dan de duur van de beroepsactiviteit van de agent onder dekmantel. Het is dus belangrijk dat het diensthoofd registers bijhoudt van de fictieve identiteiten/hoedanigheden om te vermijden dat bijvoorbeeld een door een agent gebruikte identiteit opnieuw gebruikt wordt door een ander agent binnen dezelfde rechtspersoon.

De agent die een fictieve identiteit en/of hoedanigheid gebruikt, houdt ook een logboek bij, waarin hij de data en de context van het gebruik vermeldt. Het gebruik van de fictieve identiteit kan bijvoorbeeld juridische gevolgen hebben die eventueel getraceerd moeten kunnen worden. Bijvoorbeeld : bankverrichtingen uitgevoerd met een fictieve identiteit, alsook de ondertekening van een overeenkomst…

Les missions du conseiller en sécurité de l'information ont été complétées, afin de mieux les préciser, en s'inspirant de l'article 9 de la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth.

Cependant, la Commission de la protection de la vie privée estime que le conseiller en sécurité de l'information devrait jouir d'une protection statutaire, comme celle des membres de l'organe de contrôle des informations policières (cf. article 44/7, dernier alinéa, de la loi sur la fonction de police), afin de pouvoir remplir sa fonction en toute indépendance.

Il convient cependant de constater que l'article 14, alinéa 4, de la loi organique ne contient pas d'habilitation au Roi pour régler le statut du conseiller en sécurité de l'information, mais seulement pour régler les modalités générales d'accès aux banques de données du secteur public utiles à l'exécution de leurs missions, par la présence effective d'un tel conseiller au sein des services de renseignement et de sécurité.

Relevons, pour le surplus, que le statut de personnes devant exercer pareille mission, en vertu d'autres législations, n'est, en général, pas encore réglé, à commencer par l'article 17*bis* de la loi du 8 décembre 1992 qui aurait pu constituer une base réglementaire de référence.

Le paragraphe 2 prévoit qu'en ce qui concerne la Sûreté de l'Etat, le conseiller à la sécurité des données actuellement désigné exerce la fonction de conseiller en sécurité de l'information et en protection de la vie privée, qui remplit, entre autres, la fonction de préposé à la protection des données visée à l'article 4.

Le conseiller à la sécurité des données actuel a été désigné par le ministre de la Justice, conformément 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, répondant ainsi à l'avis n° 5/2000 du 13 mars 2000 de la Commission de la protection de la vie privée et à l'avis de Conseil d'Etat rendu sur ledit arrêté.

Il verra donc sa mission élargie aux banques de données du secteur public, auxquelles les services de renseignement et de sécurité pourront avoir accès, en application de l'article 14, alinéa 4, de la loi du 30 novembre 1998.

Article 5

L'article 5 prévoit que les services de renseignement et de sécurité accèdent sans frais aux banques de données du secteur public. Cette exonération se justifie par le fait que les services de renseignement sont des services de l'Etat ayant pour mission de protéger les intérêts fondamentaux de l'Etat. Il n'est pas logique, dès lors, que l'Etat paie l'Etat pour des services rendus par l'Etat en vue de le protéger.

Chapitre IV. — *Des méthodes spécifiques et des méthodes exceptionnelles de recueil des données*

Section 1re. — Des identités et qualités fictives

Article 6

Alors que l'utilisation d'un faux nom est une méthode ordinaire, l'utilisation d'une identité ou d'une qualité fictive est liée à la création ou au recours à des personnes morales, qui est une méthode exceptionnelle décrite à l'article 18/13 de la loi du 30 novembre 1998, inséré par la loi du 4 février 2010. L'identité ou la qualité fictive couvre l'agent du service de renseignement, chargé de collecter de façon ciblée des données en rapport avec des événements, des objets, des groupements et des personnes physiques ou morales présentant un intérêt pour l'exercice des missions. Précisons que les méthodes exceptionnelles ne peuvent être mises en œuvre que dans le cadre des menaces visées à l'article 18/9, § 1er, nouveau, de la loi du 30 novembre 1998.

La personne morale, créée à l'appui des activités opérationnelles, peut avoir une durée de vie plus longue que la durée de l'activité professionnelle de l'agent sous couverture. Il importe, dès lors, que le dirigeant du service tienne des registres des identités/qualités fictives, afin d'éviter qu'une identité utilisée par un agent soit réutilisée par un autre agent au sein de la même personne morale, par exemple.

L'agent qui utilise une identité et/ou une qualité fictive tient également un journal de bord où il inscrit les dates et le contexte de l'utilisation. L'utilisation de l'identité fictive, par exemple, peut avoir des effets juridiques qui, le cas échéant, doivent pouvoir être retracés. Par exemple, des opérations bancaires effectuées sous identité fictive, ainsi que la signature d'un contrat…

De agent vermeldt in zijn logboek ook de incidenten die zich voordoen. De inlichtingenofficier die aangesteld wordt om deze uitzonderlijke methode uit te voeren, moet het diensthoofd hiervan regelmatig op de hoogte brengen. Deze informatie zal opgenomen worden in het rapport dat het diensthoofd iedere twee maanden aan de commissie voor toezicht moet bezorgen over het verloop van de uitzonderlijke methode, overeenkomstig artikel 18/13, vierde lid, nieuw, van de wet van 30 november 1998.

Dit logboek maakt het voorwerp uit van een controle :

— door het diensthoofd dat regelmatig op de hoogte gebracht wordt door de inlichtingenofficier die aangesteld is voor de aanwending van deze uitzonderlijke methode;

— door de commissie via een tweemaandelijks verslag over de evolutie van de methode, haar geadresseerd door de betrokken inlichtingen – en veiligheidsdienst ingevolge voornoemd artikel 18/13, vierde lid en waarin desbetreffende informatie geïntegreerd is.

Op vraag van de Commissie voor de bescherming van de persoonlijke levenssfeer wordt dit logboek gedurende tien jaar bewaard, nadat de fictieve identiteit of hoedanigheid niet meer actief is.

Afdeling 2. — Nadere regels voor de vernietiging van de opnamen en van de eventuele overschrijvingen en vertalingen van de communicaties

Artikel 7

Artikel 18/17, § 7, en § 4, tweede lid, nieuw, van de wet van 30 november 1998 voorziet dat de vernietiging van opnamen, eventuele overschrijvingen en vertalingen van de communicaties gebeurt onder toezicht van de commissie en van het diensthoofd of, naargelang het geval, in zijn naam, van de directeur van de operaties of van de persoon die hij hiertoe aangesteld heeft, voor de Veiligheid van de Staat, of door de officier of de burgerambtenaar die minstens de graad van commissaris heeft voor de Algemene Dienst Inlichtingen en Veiligheid, of hun afgevaardigde. De Koning dient de nadere regels voor vernietiging te bepalen. De vermelding van de vernietiging gebeurt in een speciaal register, zoals bedoeld in artikel 18/17, § 6, nieuw, van de wet van 30 november 1998.

De opnamen, de eventuele overschrijvingen of vertalingen van de communicaties kunnen vastgelegd worden op verschillende dragers, papier, geluidsbanden, CD's, DVD's, PC, USB-sticks of andere technische middelen. Rekening houdende met de technologische evolutie is het ook onmogelijk om de technische instrumenten voor vernietiging te definiëren. Wat van belang is, is dat de vernietiging iedere volgende exploitatie van de gegevens onmogelijk maakt. Ook het meest geschikte instrument om de opnamen, de eventuele overschrijvingen of vertalingen van de communicaties te vernietigen, moet beantwoorden aan de meest efficiënte technische voorwaarden die onophoudelijk evolueren. Het is op het ogenblik van de vernietiging dat de meest geschikte werkwijze gekozen zal moeten worden. De commissie zal hierop toezien door middel van controle.

Afdeling 3. — De vergoeding voor de medewerking van natuurlijke personen en rechtspersonen

Artikel 8

De tarieven voor de medewerking van de natuurlijke persoon of de rechtspersoon worden bij voorkeur bepaald op basis van de bestaande reglementaire bepalingen inzake de gerechtskosten in strafzaken.

Deze tarieven betreffen niettemin handelingen in het kader van gerechtelijke procedures die niet noodzakelijk overeenstemmen met prestaties die specifieke en uitzonderlijke methoden zouden vereisen. Daarom is ook een specifieke tariefformule voorzien, die enerzijds, voor de prestaties van de natuurlijke personen, gebaseerd is op de facturatie of een onkostennota die rekening houdt met de werkelijke kost veroorzaakt door de geleverde prestatie en anderzijds op de eventuele meerkost die veroorzaakt wordt door de medewerking van de rechtspersoon, in verhouding tot zijn normale werking. In deze laatste veronderstelling kan de rechtspersoon van mening zijn dat zijn medewerking geen enkele bijkomende kost met zich meebrengt in verhouding tot zijn normale werking. Dit is niet het geval als het gaat om een ongewone vraag die bijkomend werk en dus een meerkost met zich meebrengt.

Wanneer de specifieke tariefformule van toepassing is, richt de natuurlijke persoon of rechtspersoon die de prestatie uitgevoerd heeft, het gerechtvaardigd detail van de uitgevoerde prestatie of de meerkost, in functie van de aard van de tussenkomst, aan het diensthoofd van de betrokken dienst.

L'agent indiquera également dans son journal de bord les incidents qu'il rencontrerait. L'officier de renseignement, désigné pour mettre en oeuvre cette méthode exceptionnelle, devra en informer régulièrement le dirigeant du service. Cette information sera intégrée dans le rapport que le dirigeant du service devra faire, tous les deux mois, à la commission de surveillance sur le déroulement de la méthode exceptionnelle, conformément à l'article 18/13, alinéa 4, nouveau, de la loi du 30 novembre 1998.

Ce journal de bord fait l'objet d'un contrôle :

— par le dirigeant du service qui est informé régulièrement par l'officier de renseignement désigné pour mettre en œuvre cette méthode exceptionnelle;

— par la commission, par le biais du rapport bimestriel sur l'évolution de la méthode qui lui est adressé par le service de renseignement et de sécurité concerné, en vertu de l'art. 18/13, alinéa 4, précité lequel intègre l'information y relative.

A la demande de la Commission de la protection de la vie privée, ce journal de bord est conservé pendant dix ans, après que l'identité ou la qualité fictive ne soit plus active.

Section 2. — Des modalités de destruction des enregistrements, transcriptions et traductions éventuelles des communications

Article 7

L'article 18/17, § 7, et § 4, alinéa 2, nouveau, de la loi du 30 novembre 1998 prévoit que la destruction des enregistrements, transcriptions et traductions éventuelles des communications est opérée sous le contrôle de la commission et du dirigeant du service ou, selon le cas, en son nom, par le directeur des opérations ou la personne qu'il a désignée à cet effet, pour la Sûreté de l'Etat, l'officier ou l'agent civil, ayant au moins le grade de commissaire, pour le Service général du renseignement et de la sécurité, ou leur délégué. Il revient au Roi de fixer les modalités de la destruction. La mention de la destruction est faite dans un registre spécial, visé à l'article 18/17, § 6, nouveau, de la loi du 30 novembre 1998.

Les enregistrements, transcriptions ou traductions éventuelles des communications peuvent être fixés sur divers supports : papier, bandes magnétiques, CD audio, DVD, PC, clés USB ou autres moyens techniques. Aussi, compte tenu de l'évolution des technologies, il est impossible de figer des moyens techniques de destruction. Ce qui importe, c'est que la destruction rende impossible toute exploitation subséquente des données. Aussi, le moyen le plus approprié de détruire les enregistrements, transcriptions ou traductions éventuelles des communications doit répondre aux conditions techniques les plus efficaces, conditions qui évoluent sans cesse. C'est au moment de la destruction que le procédé le plus approprié devra être choisi. La commission, par son contrôle, y veillera.

Section 3. — La rétribution de la collaboration des personnes physiques et des personnes morales

Article 8

Les tarifs de la collaboration de la personne physique ou de la personne morale sont de préférence déterminés sur la base des dispositions règlementaires existantes relatives aux frais de justice en matière répressive.

Toutefois, ces tarifs concernent des actes intervenant dans le cadre de procédures judiciaires, qui ne correspondront pas nécessairement aux prestations que les méthodes spécifiques et exceptionnelles pourraient demander. C'est la raison pour laquelle une formule de tarification spécifique, basée, d'une part, sur la facturation ou une note de frais qui tient compte du coût réel supporté en raison de la prestation effectuée, pour les prestations des personnes physiques et, d'autre part, sur le surcoût éventuel engendré par la collaboration de la personne morale par rapport à son fonctionnement normal, est également prévue. Dans cette dernière hypothèse, la personne morale peut estimer que sa collaboration n'engendre aucun coût supplémentaire par rapport à son fonctionnement normal. Il n'en est pas de même s'il s'agit d'une demande inhabituelle suscitant un travail supplémentaire, donc un surcoût.

Lorsque la formule tarifaire spécifique est d'application, la personne physique ou la personne morale qui a effectué la prestation, adresse, au dirigeant du service concerné, le détail de la prestation effectuée ou du surcoût, dûment justifié, en fonction de la nature de l'intervention.

Het spreekt voor zich dat deze gerechtvaardigde kosten het voorwerp uitmaken van de gebruikelijke budgettaire controle overeenkomstig de gecoördineerde wetten van 17 juli 1991 op de Rijkscomptabiliteit.

Hoofdstuk V. — *Het toezicht op de specifieke en uitzonderlijke methoden*

Afdeling 1. — Nadere regels en termijnen voor de kennisgeving aan de commissie

Artikelen 9 en 10

Artikel 18/10, § 1, derde lid, nieuw, van de wet van 30 november 1998 voorziet dat het diensthoofd de commissie regelmatig op de hoogte brengt van het verloop van de uitzonderlijke methode. Onder voorbehoud van de termijn voorzien in artikel 18/13, nieuw, van de wet van 30 november 1998 brengt het diensthoofd de commissie om de twee weken en wanneer de methode beëindigd is, op de hoogte.

Hetzelfde geldt wanneer de leden van de commissie op de hoogte moeten worden gebracht van de machtiging gegeven door het diensthoofd in geval van uiterste hoogdringendheid en met de voorafgaande akkoordbevinding van de voorzitter van de commissie.

De snelste informatiemiddelen zijn voorzien : ofwel de beveiligde elektronische weg, ofwel, indien dit onmogelijk is, per drager overgemaakte informatie.

Afdeling 2. — Nadere regels voor de kennisgeving zoals bedoeld in artikel 43/3 van de wet van 30 november 1998

Artikel 11

Artikel 43/3, nieuw, van de wet van 30 november 1998 voorziet dat de maandelijkse lijsten van de specifieke maatregelen die uitgevoerd werden, onverwijld ter kennis worden gebracht van het Vast Comité I door de bevoegde overheid, net zoals het geheel aan beslissingen, adviezen en machtigingen betreffende de specifieke en uitzonderlijke methoden. De Koning staat in voor het bepalen van de nadere regels.

Voor de toepassing van artikel 43/3, eerste lid van de wet, voorziet artikel 11 dat de maandelijkse lijsten zoals bedoeld in artikel 18/3, § 2, van de wet vanaf hun ontvangst door de commissie, zullen overgemaakt worden aan het Vast Comité I.

De verschillende beslissingen, adviezen en machtigingen, zoals bedoeld in artikel 43/3, tweede lid, van de wet, zullen onverwijld en integraal door de commissie meegedeeld worden aan het Vast Comité I.

De gegevens met betrekking tot deze beslissingen, adviezen en machtigingen zullen het voorwerp uitmaken van een gestructureerde mededeling die betrekking heeft op :

— de identiteit van de overheid die de beslissing genomen heeft, het advies of de machtiging gegeven heeft;
— de datum van de beslissing, het advies of de machtiging;
— de aard van de specifieke of uitzonderlijke methode;
— de aard van de dreiging en de aard van het te vrijwaren belang;
— de graad en ernst van de dreiging;
— de evaluatie van de proportionaliteit en de subsidiariteit;
— de natuurlijke of rechtsperso(o)n(en), verenigingen of groeperingen, voorwerpen, plaatsen, gebeurtenissen of informatie die het voorwerp uitmaken van de methode;
— de hoedanigheid van advocaat, arts of journalist van de perso(o)n(en) die het voorwerp uitmaken van de methode;
— het feit dat lokalen aangewend worden voor beroepsdoeleinden of als woonplaats door een advocaat, een arts of een journalist;
— het gebruikte technische middel;
— de periode tijdens dewelke de methode uitgevoerd wordt;
— het feit dat het om een verlenging gaat.

De kennisgevingen gebeuren onder gedigitaliseerde vorm. Behoudens volstrekte onmogelijkheid of ingevolge het uitdrukkelijk verzoek van het Vast Comité I, kan de kennisgeving op een andere, door het Vast Comité I te bepalen wijze, gebeuren. Zij maken het voorwerp uit van een ontvangstbevestiging.

Afdeling 3. — Nadere regels en termijnen voor de bewaring van gegevens die ontwettig verzameld zijn door een specifieke of uitzonderlijke methode

Artikel 12

Krachtens de artikelen 18/3, § 2, tweede lid en 18/10, § 6, nieuwe, van de wet van 30 november 1998 mag de commissie op ieder ogenblik de wettigheid van een specifieke of uitzonderlijke methode controleren. Wanneer zij van mening is dat gegevens verzameld zijn in omstandigheden die de geldende wettelijke bepalingen niet respecteren, verbiedt zij de diensten om de verzamelde gegevens te exploiteren. Deze gegevens worden onder toezicht van de commissie bewaard.

Il va de soi que ces frais dûment justifiés font l'objet du contrôle budgétaire ordinaire, conformément aux lois coordonnées du 17 juillet 1991 sur la comptabilité de l'Etat.

Chapitre V. — *Du contrôle des méthodes spécifiques et exceptionnelles*

Section 1re. — Des modalités et délais d'information de la commission

Articles 9 et 10

L'article 18/10, § 1er, alinéa 3, nouveau, de la loi du 30 novembre 1998 prévoit que le fonctionnaire dirigeant informe régulièrement la commission du déroulement de la méthode exceptionnelle. Sous réserve du délai prévu à l'article 18/13, nouveau, de la loi du 30 novembre 1998, le dirigeant du service informera la commission toutes les deux semaines et lorsque la méthode prend fin.

Il en sera de même lorsque les membres de la commission doivent être informés de l'autorisation donnée par le dirigeant du service, en cas d'extrême urgence et avec l'accord préalable du président de la commission.

Les moyens d'information les plus rapides sont prévus, à savoir : soit la voie électronique sécurisée, soit, en cas d'impossibilité par ce moyen, l'information transmise par porteur.

Section 2. — Modalités pour les communications telles que visées à l'article 43/3 de la loi du 30 novembre 1998

Article 11

L'article 43/3, nouveau, de la loi du 30 novembre 1998 prévoit que les listes mensuelles des mesures spécifiques ayant été exécutées sont portées, sans délai, à la connaissance du Comité permanent R par l'autorité compétente, de même que l'ensemble des décisions, avis et autorisations concernant les méthodes spécifiques et exceptionnelles. Il revient au Roi d'en fixer les modalités.

Pour l'application de l'article 43/3, alinéa 1er, de la loi, l'article 11 prévoit que les listes mensuelles, visées à l'article 18/3, § 2 de la loi, seront adressées au Comité permanent R par la commission, dès leur réception.

En ce qui concerne les décisions, avis et autorisations divers, visés à l'article 43/3, alinéa 2, de la loi, ils seront communiqués au Comité permanent R, sans délai et intégralement, par la commission.

Les données relatives à ces décisions, avis et autorisations feront l'objet d'une communication structurée portant sur :

— l'identité de l'autorité qui a pris la décision, donné l'avis ou l'autorisation;
— la date des décision, avis, autorisation;
— la nature de la méthode spécifique ou exceptionnelle;
— la nature de la menace et de l'intérêt à préserver;
— le degré de gravité de la menace;
— l'évaluation de la proportionnalité et de la subsidiarité;
— la ou les personnes physiques ou morales, les associations ou les groupements, les objets, les lieux, les événements, les informations soumis à la méthode;
— la qualité d'avocat, médecin, journaliste de la ou des personnes soumise(s) à la méthode;
— l'indication que les locaux sont utilisés à des fins professionnelles ou comme résidence par un avocat, médecin ou journaliste;
— le moyen technique utilisé;
— la période de mise en oeuvre de la méthode;
— l'indication qu'il s'agit d'une prolongation.

Les communications s'effectueront numériquement. En cas d'impossibilité absolue ou sur demande expresse du Comité permanent R, la communication pourra se faire d'une autre manière déterminée par le Comité permanent R. Elles feront l'objet d'un accusé de réception.

Section 3. — Des modalités et délais de conservation des données illégalement recueillies par une méthode spécifique ou exceptionnelle

Article 12

En vertu des articles 18/3, § 2, alinéa 2, et 18/10, § 6, nouveaux, de la loi du 30 novembre 1998, la commission peut contrôler, à tout moment, la légalité d'une méthode spécifique ou exceptionnelle. Lorsqu'elle estime que des données ont été recueillies dans des conditions qui ne respectent pas les dispositions légales en vigueur, elle interdit aux services d'exploiter les données ainsi recueillies. Celles-ci sont conservées sous le contrôle de la commission.

Artikel 12 voorziet dat deze gegevens onverwijld in een verzegelde omslag bewaard worden op een beveiligde plaats die door de commissie bepaald wordt in overleg met het betrokken diensthoofd om te vermijden dat ze nog geëxploiteerd worden. De geïnformatiseerde gegevens worden, totdat het Vast Comité I zich uitgesproken heeft over de wettelijkheid ervan, onleesbaar gemaakt met behulp van de meest geschikte technische methoden op het ogenblik van de operatie, zodat deze gegevens onmogelijk nog geëxploiteerd kunnen worden door de inlichtingen- en veiligheidsdiensten. Overeenkomstig het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer wordt gepreciseerd dat de geïnformatiseerde gegevens tijdelijk ontoegankelijk worden gemaakt in afwachting van de definitieve beslissing van het Vast Comité I en naar het voorbeeld van wat voorzien is voor de « papieren » gegevens, met uitzondering voor de raadgever inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer die, minstens, toegang moet kunnen nemen, weze het om de gegevens terug toegankelijk te maken in geval van een beslissing in die zin van het Vast Comité I.

L'article 12 prévoit que ces données sont conservées, sans délai, sous scellé, dans un lieu sécurisé qu'elle désigne en concertation avec le dirigeant du service concerné, afin d'éviter leur exploitation. Les données informatisées sont, quant à elles, rendues illisibles au moyen d'un procédé technique, le plus approprié au moment de l'opération, de sorte qu'il ne soit pas possible pour les services de renseignement et de sécurité d'exploiter ces données, jusqu'à ce que le Comité permanent R se soit prononcé sur leur légalité. Conformément à l'avis de la Commission de la protection de la vie privée, il est précisé que les données informatisées sont rendues temporairement inaccessibles, dans l'attente de la décision définitive du Comité permanent R, à l'instar de ce qui est prévu pour les données « papier », sauf pour le conseiller en sécurité de l'information et en protection de la vie privée, qui doit, à tout le moins, pouvoir y avoir accès, ne fût-ce que pour rendre les données à nouveau accessibles, en cas de décision de Comité permanent R en ce sens.

Afdeling 4. — Nadere regels voor de vernietiging van gegevens die ontwettig verzameld zijn door een specifieke of uitzonderlijke methode

Artikel 13

Het Vast Comité I beslist om gegevens die door een onwettige uitzonderlijke of specifieke methode verzameld zijn, te vernietigen.

Dit Comité deelt zijn beslissing o.a. aan het betrokken diensthoofd mee. Er zal zo snel mogelijk, en ten laatste een maand na deze mededeling, overgegaan worden tot de vernietiging van de gegevens. De vernietiging wordt uitgevoerd met behulp van de meest geschikte technische methoden, onder de controle van een lid van de bestuurlijke commissie voor toezicht en het betrokken diensthoofd of de persoon die hij hiertoe aanstelt. Deze personen en een veiligheidsofficier van de betrokken dienst medeondertekenen het rapport dat opgesteld is door de persoon die de vernietiging uitvoert. Het Vast Comité I wordt op de hoogte gebracht van deze vernietiging.

Section 4. — Des modalités de destruction des données illégalement recueillies par une méthode spécifique ou exceptionnelle

Article 13

La décision de détruire les données recueillies par une méthode spécifique ou exceptionnelle illégale appartient au Comité permanent R.

Celui-ci communique sa décision, entre autres, au dirigeant du service concerné. Il sera procédé à la destruction des données le plus vite possible et, au plus tard, un mois après cette communication. La destruction est opérée, au moyen des procédés techniques les plus appropriés, sous le contrôle d'un membre de la commission administrative de surveillance et du dirigeant du service concerné ou de la personne qu'il désigne à cet effet. Ceux-ci et un officier de sécurité du service concerné contresignent le rapport rédigé par l'auteur de la destruction. Le Comité permanent R est avisé de cette destruction.

Hoofdstuk VI. — *Adiëring van het Vast Comité I door de Commissie voor de bescherming van de persoonlijke levenssfeer op grond van artikel 43/4 van de wet van 30 november 1998*

Artikel 14

Het Vast Comité I handelt namelijk op vraag van de Commissie voor de bescherming van de persoonlijke levenssfeer. De Koning dient de nadere regels te bepalen voor de vatting van dit Comité.

Zo kan deze commissie als ze, in het kader van een controle die door de Commissie voor de bescherming van de persoonlijke levenssfeer uitgevoerd wordt ingevolge een vraag van onrechtstreekse toegang, een redelijke achterdocht heeft dat persoonlijke gegevens verzameld werden door een specifieke of uitzonderlijke methode ondanks de regels vervat in de wet van 30 november 1998, een gemotiveerde vraag aan het Vast Comité I richten.

De vraag omvat volgende elementen :

— de betrokken dienst;

— de duiding van de beoogde gegevens;

— de elementen die voor de achterdocht gezorgd hebben dat de gegevens verzameld werden door een specifieke of uitzonderlijke methode ondanks de regels van de wet van 30 november 1998.

Zij wordt via een aangetekende zending of op een andere wijze waarover een onderling akkoord bestaat, overgemaakt met naleving van de regels van overdracht van geclassificeerde informatie.

Chapitre VI. — *La saisine du Comité permanent R par la Commission de la protection de la vie privée en vertu de l'article 43/4 de la loi du 30 novembre 1998*

Article 14

Le Comité permanent R agit, notamment, à la demande de la Commission de la protection de la vie privée. Il revient au Roi de déterminer les modalités de la saisine dudit Comité.

C'est ainsi que si, dans le cadre d'une vérification effectuée par la Commission de la protection de la vie privée, à la suite d'une demande d'accès indirect, cette Commission a une suspicion raisonnable que des données à caractère personnel ont été recueillies par une méthode spécifique ou exceptionnelle au mépris des règles contenues dans la loi du 30 novembre 1998, elle peut adresser une demande motivée au Comité Permanent R.

La demande comprend les éléments suivants :

— le service concerné;

— l'indication des données visées;

— les éléments qui ont fait naître la suspicion que les données ont été recueillies par une méthode spécifique ou exceptionnelle et au mépris des règles de la loi du 30 novembre 1998.

Elle est transmise par envoi recommandé ou d'une autre manière déterminée de commun accord, dans le respect des règles de transmission des informations classifiées.

Hoofdstuk VII. — *Eindbepalingen*

Artikel 15

Overeenkomstig het advies van de Raad van State, wordt een artikel 15 tot uitvoering ingevoegd.

Chapitre VII. — *Dispositions finales*

Article 15

Conformément à l'avis du Conseil d'Etat, un article 15 d'exécution est ajouté.

Artikel 16

Artikel 16 voorziet dat het koninklijk besluit in werking zal treden op de dag van de publicatie in het *Belgisch Staatsblad*. Het is immers van belang dat de wet, die reeds van kracht is, zo snel mogelijk werkzaam wordt.

Wij hebben de eer te zijn,

Sire,
Van Uwe Majesteit,
de zeer eerbiedige
en zeer getrouwe dienaars,

De Minister van Justitie,
S. DECLERCK

De Minister van Landsverdediging,
P. DE CREM

ADVIES NR. 24/2010
VAN 30 JUNI 2010

Betreft : Voorontwerp van koninklijk besluit houdende uitvoering van diverse bepalingen van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (hierna WVP), inzonderheid artikel 29;

Gelet op het verzoek om advies van de heer Stefaan De Clerck, Minister van Justitie, ontvangen op 31 mei 2010;

Gelet op het verslag van de heer Frank Schuermans;

Brengt op 30 juni 2010 het volgend advies uit :

A. Inleiding

1. De Minister van Justitie heeft op 31 mei 2010 aan de Commissie een advies gevraagd betreffende een ontwerp van koninklijk besluit houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

2. Gelet op de aanneming van de wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten, werden aan de Koning verschillende bevoegdheden overgelaten teneinde uitvoeringsmaatregelen te nemen voor de nieuwe, gewijzigde bepalingen van de organieke Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

B. Analyse van het ontwerp van koninklijk besluit

3. In de aanhef zou het opportuun zijn het volgende te formuleren : « Gelet op het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, gegeven op 30 juni 2010 ». Inderdaad, het onderzoek van de Commissie bleef niet uitsluitend beperkt tot de artikelen 12, 13 en 14 maar had betrekking op het volledige ontwerp van koninklijk besluit.

Gebruik van een valse naam

(artikel 13/1 van de wet van 30 november 1998, artikel 2 van het ontwerp van koninklijk besluit).

4. Het diensthoofd van de inlichtingen- en veiligheidsdienst houdt een specifiek logboek bij met daarin :

— de lijst met gebruikte valse namen en het verband met de agent die deze gebruikt;

— de data, de context en, desgevallend, de incidenten die plaatsgevonden hebben bij het gebruik van de valse naam.

Toegang tot de gegevensbanken van de openbare sector

(artikel 14, 4e lid van de wet van 30 november 1998, artikel 3, van het ontwerp van koninklijk besluit)

5. Indien de inlichtingen- en veiligheidsdienst rechtstreeks toegang heeft tot de databank :

— wordt een nominatieve lijst bijgehouden met de personen die gemachtigd zijn om toegang te hebben en wordt deze lijst permanent ter beschikking gehouden van de Commissie;

— wordt een logbestand (m.a.w. een logging van de toegangen tot de databank) gegenereerd bij iedere raadpleging. Dit wordt gedurende minimum 12 maanden bewaard.

Article 16

L'article 16 prévoit que la date d'entrée en vigueur de l'arrêté royal aura lieu le jour de sa publication au *Moniteur belge*. En effet, il importe que la loi qui est déjà entrée en vigueur soit rendue effective le plus rapidement possible.

Nous avons l'honneur d'être,

Sire,
de Votre Majesté,
les très respectueux
et très fidèles serviteurs,

Le Ministre de la Justice,
S. DECLERCK

Le Ministre de la Défense,
P. DE CREM

AVIS N° 24/2010
DU 30 JUIN 2010

Objet : Projet d'arrêté royal portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (CO/A/2010/022)

La Commission de la protection de la vie privée (ci-après la Commission);

Vu la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (ci-après LVP), en particulier l'article 29;

Vu la demande d'avis de M. Stefaan De Clerck, Ministre de la Justice, reçue le 31 mai 2010;

Vu le rapport de M. Frank Schuermans;

Emet, le 30 juin 2010, l'avis suivant :

A. Introduction

1. Le 31 mai 2010, le Ministre de la Justice a demandé à la Commission d'émettre un avis concernant un projet d'arrêté royal portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

2. Vu l'adoption de la loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité, plusieurs habilitations ont été laissées au Roi afin de prendre des mesures d'exécution des nouvelles dispositions modifiées de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

B. Analyse du projet d'arrêté royal

3. Dans les visas, il serait opportun de libeller de la manière suivante : ″vu l'avis de la Commission de la protection de la vie privée, donné le 30 juin 2010″. En effet, l'examen de la Commission ne s'est pas limité aux seuls articles 12, 13 et 14 mais a porté sur l'entièreté du projet d'arrêté royal.

Utilisation d'un faux nom

(article 13/1 de la loi du 30 novembre 1998, article 2 du projet d'arrêté royal).

4. Le dirigeant du service de renseignement et de sécurité tient à jour un journal de bord spécifique dans lequel on trouvera :

— la liste des faux noms utilisés et le lien avec l'agent qui les utilise;

— les dates, contexte et, le cas échéant, les incidents survenus concernant l'utilisation du faux nom.

Accès aux banques de données publiques

(article 14, alinéa 4 de la loi du 30 novembre 1998, article 3, du projet d'arrêté royal).

5. Si le service de renseignement et de sécurité a un accès direct à la banque de données :

— une liste nominative des personnes habilitées à accéder est tenue en permanence à la disposition de la Commission;

— un fichier log (c'est-à-dire une journalisation des accès à la banque de données) est généré à chaque demande de consultation. Il est conservé 12 mois au minimum.

6. Artikel 14, 4e lid van de organieke wet laat in het midden of de toegang tot de gegevensbanken van de openbare sector ook heimelijk kunnen geschieden. Derhalve stelt zich de vraag of het niet opportuun is in principe de beheerder van de gegevensbank op de hoogte te stellen van de raadpleging telkens dergelijke raadpleging door de inlichtingendiensten gebeurt teneinde het transparantiebeginsel te eerbiedigen. Een notificatie in die zin lijkt immers noodzakelijk. Slechts met een gedegen motivering zou hiervan dan kunnen afgeweken worden, desgevallend na advies van de bestuurlijke commissie, nu een heimelijke raadpleging van andermans databank niet voor de hand liggend lijkt. Uiteraard dienen de nodige maatregelen te worden genomen opdat dergelijke notificatie het heimelijk karakter van het inlichtingenwerk niet in het gedrang zou brengen wat bijvoorbeeld zou kunnen door slechts één of enkele personen te verwittigen en andere technische maatregelen. Deze opmerking klemt des te meer nu, in het geval er geen rechtstreekse toegang voorzien is, de agent van de inlichtingendienst zijn legitimatiekaart dient voor te leggen aan de beheerder van de databank (cf. punt 7).

De voorziene termijn van 12 maanden lijkt wel een minimum. De commissie beveelt aan loggegevens gedurende 10 jaar bij te houden, a fortiori wanneer het om heimelijke consultaties van andere databestanden gaat.

Deze termijn van 10 jaar is gelijkaardig aan wat gebruikelijk is in de sociale sector en opgelegd wordt door de afdeling sociale zekerheid van het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid. Investeringsgewijs betekent dit slechts een kleine meerinspanning en deze termijn laat met veel meer zekerheid toe misbruiken nog op een nuttige manier te kunnen achterhalen tijdens een latere controle of inspectie.

7. Indien de inlichtingen- en veiligheidsdienst geen rechtstreekse toegang heeft tot de databank worden de gegevens onmiddellijk aan de agent van de inlichtingen- en veiligheidsdienst meegedeeld op vertoon van zijn legitimatiekaart.

De Commissie beveelt aan dat naar analogie van wat voorzien is voor de rechtstreekse toegang, een logbestand met de aanvragen zou bijgehouden worden door de beheerder van de databank en dat een schriftelijk spoor van deze raadpleging eveneens zou bewaard worden op het niveau van de inlichtingen- en veiligheidsdienst. Inderdaad, ook deze raadplegingen moeten evengoed gelogd worden.

8. Een veiligheidsconsulent wordt aangeduid in de schoot van elke inlichtingen- en veiligheidsdienst : hij is belast met de naleving van de wet bij iedere aanvraag van gegevens en voor het nemen van alle nuttige maatregelen teneinde de veiligheid van de geregistreerde informatie te verzekeren (artikel 4 van het ontwerp van koninklijk besluit).

De Commissie benadrukt ook het belang van de onafhankelijke positie die de aangestelde voor de gegevensbescherming of veiligheidsconsulent dient te hebben in de organisatie. Hij dient enkel verantwoording af te leggen en rapporteert aan het hoofd van de inlichtingen - of veiligheidsdienst (met name de administrateur-generaal van de Veiligheid van de Staat of de Chef van de Algemene Dienst Inlichtingen en Veiligheid). Hij moet ook de mogelijkheid hebben, zonder vrees op sancties of andere negatieve gevolgen, van rechtstreeks te rapporteren aan de bestuurlijke commissie en de bestuurlijke commissie of het Comité I moet in de mogelijkheid zijn betrokkene rechtstreeks te bevragen. Belangrijk is tot slot dat betrokkene een zekere statutaire bescherming geniet zoals dat bijvoorbeeld het geval is voor de leden van het Controleorgaan voor de politionele informatie (cf. art. 44/7, laatste lid van de Wet van 5 augustus 1992 op het Politieambt) zodat hij of zij in volle onafhankelijkheid zijn functie kan vervullen.

De Commissie merkt op dat een verschillende terminologie wordt gebruikt (zowel in het Frans als in het Nederlands) zodat het risico ontstaat op een uiteenlopende interpretatie : het ontwerp van koninklijk besluit voert een « raadsman voor de veiligheid van de gegevens » in (in het Frans : « conseiller à la sécurité des données »). De Commissie beveelt veeleer aan de formulering van artikel 4 van het ontwerp van Koninklijk besluit aan te passen aan de bestaande terminologie : hetzij door zich te baseren op artikel 17*bis* van de WVP (aangestelde voor de gegevensbescherming – préposé à la protection des données); hetzij door zich te baseren op artikel 10 van de Wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen (consulent voor de informatieveiligheid – consultant en sécurité de l'information).

9. Welke ook de benaming weze die uiteindelijk door de auteurs van het ontwerp van Koninklijk besluit zal weerhouden worden, zal deze « raadsman voor de veiligheid » de facto eveneens de functie uitoefenen van « aangestelde voor de gegevensbescherming » (in het Frans : préposé à la protection des données) in de zin van artikel 17*bis* van de WVP.

6. L'article 14, 4ème alinéa de la loi organique passe sous silence le fait de savoir si l'accès aux banques de données du secteur public peut également se faire de manière secrète. Par conséquent, la question se pose de savoir s'il n'est pas opportun d'informer en principe le gestionnaire de la banque de données de la consultation chaque fois qu'une telle consultation est effectuée par les services de renseignement afin de respecter le principe de transparence. Une notification en ce sens semble en effet nécessaire. Seule une motivation solide pourrait permettre une dérogation à ce principe, le cas échéant, après avis de la commission administrative, étant donné qu'une consultation secrète de la banque de données d'autrui ne semble pas évidente. Les mesures nécessaires doivent en effet être prises afin qu'une telle notification ne compromette pas le caractère secret du travail de renseignement, ce qui serait par exemple possible en n'avertissant qu'une ou quelques personnes et en prenant d'autres mesures techniques. Cette remarque est d'autant moins logique que dans le cas où aucun accès direct n'est prévu, l'agent du service de renseignement doit présenter sa carte de légitimation au gestionnaire de la banque de données (cf. le point 7).

Le délai prévu de 12 mois semble toutefois être un minimum. La Commission recommande de conserver les données de journalisation pendant 10 ans, a fortiori lorsqu'il s'agit de consultations secrètes d'autres bases de données.

Ce délai de 10 ans est comparable à celui appliqué habituellement dans le secteur social et imposé par la section Sécurité sociale du Comité sectoriel de la Sécurité sociale et de la Santé. Du point de vue de l'investissement, cela ne représente qu'un petit effort supplémentaire et ce délai permet de pouvoir détecter, avec bien plus de certitude, des abus lors d'une inspection ou d'un contrôle ultérieur.

7. Si le service de renseignement et de sécurité n'a pas d'accès direct à la banque de données, les données sont communiquées immédiatement à l'agent du service de renseignement et de sécurité, sur présentation de sa carte de légitimation.

La Commission recommande qu'à l'instar de ce qui est prévu pour l'accès direct, une journalisation des demandes soit enregistrée par le gestionnaire de la base de données et qu'une trace écrite de cette consultation apparaisse également au niveau du service de renseignement et de sécurité. Ces consultations doivent naturellement également faire l'objet d'une journalisation.

8. Un conseiller à la sécurité est désigné au sein de chaque service de renseignement et de sécurité : il est chargé de garantir le respect de la loi lors de toute demande de données et de prendre toutes les mesures utiles afin d'assurer la sécurité des informations enregistrées (article 4 du projet d'arrêté royal).

La Commission insiste également sur l'importance de la position indépendante que le préposé à la protection des données ou le conseiller en sécurité doit avoir au sein de l'organisation. Il ne doit rendre des comptes et faire rapport qu'au chef du renseignement – ou du service de sécurité (à savoir l'administrateur général de la Sûreté de l'Etat ou le Chef du Service Général du Renseignement et de la Sécurité). Il doit aussi avoir la possibilité, sans crainte de sanctions ou d'autres conséquences négatives, de faire rapport directement à la commission administrative et cette dernière ou le Comité R doit pouvoir interroger directement l'intéressé. Enfin, il importe que l'intéressé jouisse d'une certaine protection statutaire comme c'est par exemple le cas pour les membres de l'organe de contrôle des informations policières (cf. article 44/7, dernier alinéa de la loi du 5 août 1992 sur la fonction de police) de manière à pouvoir remplir sa fonction en toute indépendance.

La Commission note qu'une terminologie différente est employée (tant en français qu'en néerlandais), au risque de créer éventuellement une divergence d'interprétation : le projet d'arrêté royal institue un ″conseiller à la sécurité des données″. La Commission recommande plutôt d'aligner le libellé de l'article 4 du projet d'arrêté royal sur la terminologie existante : soit en se basant sur l'article 17*bis* de la LVP (préposé à la protection des données); soit en se basant sur l'article 10 de la loi du 8 aout 1983 organisant un registre national des personnes physiques (conseiller en sécurité de l'information).

9. Quelle que soit la dénomination finalement retenue par les auteurs du projet d'arrêté royal, ce ″conseiller à la sécurité″ remplira aussi de facto la fonction de ″préposé à la protection des données″ au sens de l'article 17*bis* de la LVP.

Identiteit en fictieve hoedanigheid

(artikel 18/13 van de wet van 30 november 1998, artikel 6 van het ontwerp van koninklijk besluit)

10. Het diensthoofd van de inlichtingen- en veiligheidsdienst houdt een specifiek logboek bij met daarin :

— de lijst met gebruikte fictieve identiteiten en hoedanigheden en het verband met de agent die deze gebruikt;

— de data, de context en, desgevallend, de incidenten die plaatsgevonden hebben bij het gebruik van deze fictieve identiteiten en hoedanigheden.

De Commissie zou eveneens graag zien dat het logboek minstens 10 jaar bewaard wordt nadat de FIK niet meer actief is (cf. randnr. 6).

Vernietiging van opnamen van communicaties

(artikel 18/17 van de wet van 30 november 1998, artikel 7 van het ontwerp van koninklijk besluit)

11. De vernietiging zal gebeuren met behulp van de meest geschikte technische methodes, rekening houdend met de evolutie van de technologie ter zake, zodat ze onmogelijk nog geëxploiteerd kunnen worden.

Vergoeding voor de medewerking met de inlichtingendiensten

(artikel 18/18 van de wet van 30 november 1998, artikel 8 van het ontwerp van koninklijk besluit)

12. Deze bepalingen geven geen aanleiding tot opmerkingen.

Toezicht op de uitzonderlijke en specifieke methoden

(artikelen 43/1 en 18/10 van de wet van 30 november 1998, artikel 9 van het ontwerp van koninklijk besluit)

13. Een onafhankelijke administratieve *ad hoc* commissie wordt door de wet belast met het toezicht op de uitzonderlijke en specifieke methoden voor inzameling van gegevens door de inlichtingen- en veiligheidsdiensten (artikel 43/1).

14. Deze commissie wordt regelmatig (via beveiligde elektronische weg) geïnformeerd over het verloop van de uitzonderlijke methoden (artikel 9 1ste lid van het ontwerp van koninklijk besluit). Bovendien moet iedere uitwisseling van beslissingen of machtigingen – en in het algemeen van elk document - tussen deze commissie en de inlichtingen- en veiligheidsdienst gebeuren volgens de regels en richtlijnen betreffende de overdracht van geclassificeerde informatie krachtens de wet van 11 december 1998 (artikel 11, 6de lid van het ontwerp van koninklijk besluit).

15. De gegevens die verzameld worden in omstandigheden die de geldende wettelijke bepalingen niet respecteren, worden onverwijld, met het oog op hun bewaring, in een verzegelde omslag geplaatst op een beveiligde plaats die door de commissie bepaald wordt (bedoeld in artikel 43/3). In afwachting van de beslissing van het Comité I (overeenkomstig artikel 43/6, § 1, van de wet van 30 november 1998), worden de gegevens in elektronische vorm onleesbaar gemaakt zodat zij niet langer geëxploiteerd kunnen worden (artikel 12 van het ontwerp van koninklijk besluit)

16. De vernietiging van deze onwettig verkregen gegevens gebeurt onder toezicht van de commissie (bedoeld in artikel 43/3) en met behulp van de meest geschikte technische methodes, rekening houdend met de evolutie van de technologie ter zake, zodat ze onmogelijk nog geëxploiteerd kunnen worden. Een vernietigingsrapport wordt hiertoe opgesteld (artikel 13 van het ontwerp van koninklijk besluit).

17. De Commissie beveelt aan artikel 12 van het ontwerp van koninklijk besluit beter te formuleren : de « papieren » gegevens worden op een beveiligde wijze bewaard zonder mogelijkheid op toegang. Hetzelfde zou moeten gelden voor de elektronische gegevens.

Er moet ook worden voorzien dat deze gegevens ontcijferd kunnen worden (opnieuw leesbaar gemaakt) indien het Comité I een gunstige beslissing neemt met betrekking tot de gebruikte methode.

Identité et la qualité fictive

(article 18/13 de la loi du 30 novembre 1998, article 6 du projet d'arrêté royal).

10. Le dirigeant du service de renseignement et de sécurité tient à jour un journal de bord spécifique dans lequel on trouvera :

— la liste des identités et qualités fictives utilisées et le lien avec l'agent qui les utilise;

— les dates, contexte et, le cas échéant, les incidents survenus concernant l'utilisation de ces identités et qualités fictives.

La Commission aimerait également que le journal de bord soit conservé au moins 10 ans après que l'identité et la qualité fictive ne soit plus active (cf. point 6).

Destruction des enregistrements des communications

(article 18/17 de la loi du 30 novembre 1998, article 7 du projet d'arrêté royal).

11. La destruction sera opérée au moyen des procédés techniques les plus appropriés compte tenu de l'évolution de la technologie en la matière, de sorte qu'il ne soit plus possible d'exploiter les données.

Rétribution de la collaboration avec les services de renseignements

(article 18/18 de la loi du 30 novembre 1998, article 8 du projet d'arrêté royal).

12. Ces dispositions n'appellent pas de remarque.

Contrôle des méthodes spécifiques et exceptionnelles

(articles 43/1 et 18/10 de la loi du 30 novembre 1998, article 9 du projet d'arrêté royal).

13. Une Commission indépendante administrative *ad hoc* est chargée par la loi de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité (article 43/1).

14. Cette Commission est régulièrement informée (par voie électronique sécurisée) du déroulement des méthodes exceptionnelles (article 9, alinéa 1er, du projet d'arrêté royal). En outre, toute décision ou autorisation – et de manière générale tout document – échangé entre cette Commission et le service de renseignement et de sécurité s'effectue dans le respect des règles et directives concernant le transfert d'informations classifiées en vertu de la loi du 11 décembre 1998 (article 11, alinéa 6, du projet d'arrêté royal).

15. Les données recueillies dans des conditions qui ne respectent pas les dispositions légales en vigueur sont placées sous scellé, sans délai, en vue de leur conservation, dans un lieu sécurisé désigné par la Commission (visée à l'article 43/3). En attendant la décision du Comité R (conformément à l'article 43/6, § 1er, de la loi du 30 novembre 1998), les données sous forme électronique sont rendues illisibles de sorte qu'il ne soit plus possible de les exploiter (article 12 du projet d'arrêté royal).

16. La destruction de ces données illégalement recueillies s'effectue sous le contrôle de la Commission (visée à l'article 43/3) et au moyen des procédés techniques les plus appropriés compte tenu de l'évolution de la technologie en la matière, de sorte qu'il ne soit plus possible d'exploiter les données. Un rapport de destruction est rédigé à cet effet (article 13 du projet d'arrêté royal).

17. la Commission recommande un meilleur libellé de l'article 12 du projet d'arrêté royal : les données ″papier″ sont conservées de manière sécurisée sans possibilité d'accès. Il devrait en être de même pour les données électroniques.

Il faut également prévoir que ces données puissent être décryptées (rendues à nouveau lisibles) si le Comité R adopte une décision favorable concernant la méthode utilisée.

Bevoegdheid van het Comité I en de CBPL

(artikel 14 van het ontwerp van koninklijk besluit).

18. In het raam van het onderzoek van dossiers op basis van artikel 13 van de WVP (onrechtstreekse toegang tot gegevensverwerkingen uitgevoerd door de politiediensten of door de inlichtingen- en veiligheidsdiensten), kan de Commissie zich tot het Comité I richten volgens de volgende procedure :

— een gemotiveerde aanvraag (en ingediend volgens de regels betreffende de overdracht van geclassificeerde informatie);

— ondersteund door een redelijk vermoeden;

— dat de persoonsgegevens verkregen werden via een uitzonderlijke of specifieke methode;

— en met miskenning van de wet van 30 november 1998.

19. De Commissie zal dus in het raam van het onderzoek van dossiers op basis van artikel 13 van de WVP de noodzakelijke controles kunnen verrichten met kennis van zaken.

20. De Commissie merkt op dat de toegang tot *a priori* wettelijk verkregen gegevens steeds mogelijk blijft, zonder bijzondere procedure, via een vraag aan de betrokken inlichtingen- en veiligheidsdienst (artikel 32 van de WVP).

Om deze redenen,

Gelet op de opmerkingen die werden geformuleerd in onderhavig advies, verstrekt de Commissie voor de bescherming van de persoonlijke levenssfeer een gunstig advies over het ontwerp van koninklijk besluit, mits rekening wordt gehouden met haar opmerkingen in de punten 3, 6, 7, 8 en 17.

Voor de Administrateur m.v., De Voorzitter,

(get.) Patrick Van Wouwe (get.) Willem Debeuckelaere

Compétence du Comité R et de la CPVP

(article 14 du projet d'arrêté royal).

18. Dans le cadre d'examen de dossiers sur base de l'article 13 de la LVP (accès indirect aux traitements de données générés par les services de police ou par les services de renseignement et de sécurité), la Commission peut s'adresser au Comité R selon la procédure suivante :

— une demande motivée (et transmise selon les règles de transfert d'informations classifiées);

— étayée par une suspicion raisonnable;

— que des données à caractère personnel sont recueillies via une méthode spécifique ou exceptionnelle;

— et au mépris de la loi du 30 novembre 1998.

19. La Commission pourra donc, dans le cadre d'examen de dossiers sur base de l'article 13 de la LVP, effectuer en toute connaissance de cause, les vérifications nécessaires.

20. La Commission note que l'accès aux données recueillies *a priori* légalement reste toujours possible, sans procédure particulière, par une demande au service de renseignement et de sécurité concerné (article 32 de la LVP).

Par ces motifs,

Vu les remarques formulées dans le présent avis, la Commission de la protection de la vie privée émet, moyennant le respect de ses observations aux points 3, 6, 7 et 17 du présent avis, un avis favorable quant au contenu actuel du projet d'arrêté royal.

Pour l'Administrateur e.c., Le Président,

(signé) Patrick Van Wouwe (signé) Willem Debeuckelaere

12 OKTOBER 2010. — Koninklijk besluit houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten

ALBERT II, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Gelet op de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, de artikelen 13/1, § 1, 14, vierde lid, 18/3, § 2, vierde lid, 18/10, § 1, derde lid, § 4, eerste lid en § 6, vierde lid, 18/13, tweede lid, 18/17, § 7, 18/18, 43/3, 43/4, eerste lid en 43/6, § 1, eerste lid, ingevoegd bij de wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten;

Gelet op het advies van de Inspecteur van Financiën geaccrediteerd bij de minister van Justitie, gegeven op 17 mei 2010 en 4 augustus 2010;

Gelet op het advies van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, op de artikelen 13 en 14, gegeven op 21 mei 2010;

Gelet op het advies van de Inspecteur van Financiën geaccrediteerd bij de minister van Landsverdediging, gegeven op 25 mei 2010;

Gelet op de akkoordbevinding van de Staatssecretaris voor Begroting, gegeven op 4 juni 2010;

Gelet op advies nr. 24/2010 van de Commissie voor de bescherming van de persoonlijke levenssfeer, gegeven op 30 juni 2010;

Gelet op advies nr. 48.659/2/V van de Raad van State, gegeven op 1 september 2010 met toepassing van artikel 84, § 1, eerste lid, 1°, 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 Landsverdediging en op het advies van de in Raad vergaderde ministers,

Hebben Wij besloten en besluiten Wij :

HOOFDSTUK I. — *Definities*

Artikel 1. Voor de toepassing van dit besluit wordt verstaan onder :

1° « wet van 30 november 1998 » : de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

2° « wet van 11 december 1998 » : de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

3° « wet van 8 december 1992 » : de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

12 OCTOBRE 2010. — Arrêté royal portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

ALBERT II, Roi des Belges,

A tous, présents et à venir, Salut.

Vu la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, les articles 13/1, § 1er, 14, alinéa 4, 18/3, § 2, alinéa 4, 18/10, § 1er, alinéa 3, § 4, alinéa 1er et § 6, alinéa 4, 18/13, alinéa 2, 18/17, § 7, 18/18, 43/3, 43/4, alinéa 1er et 43/6, § 1er, alinéa 1er, insérés par la loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité;

Vu l'avis de l'Inspecteur des Finances accrédité auprès du ministre de la Justice, donné les 17 mai 2010 et 4 août 2010;

Vu l'avis du Comité permanent de contrôle des services de renseignement et de sécurité sur les articles 13 et 14, donné le 21 mai 2010;

Vu l'avis de l'Inspecteur des Finances accrédité auprès du ministre de la Défense, donné le 25 mai 2010;

Vu l'accord du Secrétaire d'Etat au Budget, donné le 4 juin 2010;

Vu l'avis n° 24/2010 de la Commission de la protection de la vie privée, donné le 30 juin 2010;

Vu l'avis n° 48.659/2/V du Conseil d'Etat, donné le 1er septembre 2010, en application de l'article 84, § 1er, alinéa 1er, 1°, 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 et de l'avis des ministres qui en ont délibéré en Conseil,

Nous avons arrêté et arrêtons :

CHAPITRE 1er. — *Définitions*

Article 1er. Pour l'application du présent arrêté, on entend par :

1° « loi du 30 novembre 1998 » : la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

2° « loi du 11 décembre 1998 » : la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

3° « loi du 8 décembre 1992 » : la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

HOOFDSTUK II. — *Uitoefening van inlichtingen- en veiligheidsopdrachten - Gebruik van een valse naam*

Art. 2. Voor de toepassing van artikel 13/1, § 1, van de wet van 30 november 1998 houdt het hoofd van de betrokken inlichtingen- en veiligheidsdienst of de persoon die hij hiertoe aanstelt, lijsten bij met de valse namen die het verband vermelden met de agent die deze gebruikt.

De agent bedoeld in het eerste lid, vermeldt in een logboek dat hiertoe bijgehouden wordt, het gebruik van de valse naam, de data, de context en, desgevallend, de incidenten die plaatsgevonden hebben.

HOOFDSTUK III. — *Gewone methoden voor het verzamelen van gegevens - Toegang tot de gegevensbanken van de openbare sector*

Art. 3. § 1. Voor de toepassing van artikel 14, vierde lid, van de wet van 30 november 1998, wanneer de inlichtingen- en veiligheidsdiensten kunnen beschikken over rechtstreekse toegang tot een gegevensbank van de openbare sector die persoonsgegevens bevat, houdt het betrokken diensthoofd permanent de nominatieve lijst van de personen die gemachtigd zijn om toegang te hebben tot de gegevensbank ter beschikking van de Commissie voor de bescherming van de persoonlijke levenssfeer, met vermelding van hun titel en hun functie.

Bij iedere aanvraag tot raadpleging van een gegevensbank wordt de identiteit van de aanvrager opgetekend in een controlesysteem binnen de betrokken inlichtingen- en veiligheidsdienst. Deze informatie wordt tien jaar bewaard.

§ 2. Wanneer de rechtstreekse toegang tot de gegevensbanken die persoonsgegevens bevatten onmogelijk is, wordt de informatie onmiddellijk aan de agent van de inlichtingen- en veiligheidsdienst meegedeeld, op vertoon van zijn legitimatiekaart.

De informatie wordt in een begrijpelijke vorm meegedeeld en geeft op exacte wijze alle gegevens met betrekking tot de betrokken persoon weer.

De aanvraag die ingediend wordt door een persoon die niet aan de in het eerste lid vereiste formaliteiten voldoet, wordt niet in overweging genomen.

§ 3. De toegang tot de gegevensbanken die geen persoonsgegevens bevatten, wordt geregeld op grond van gesloten akkoorden en op de door de verantwoordelijke overheden bepaalde wijze.

Art. 4. § 1. Door de bevoegde minister wordt op voordracht van het betrokken diensthoofd een raadgever informatieveiligheid en bescherming van de persoonlijke levenssfeer, die onder meer de functie vervult van aangestelde voor de gegevensbescherming, zoals bedoeld in artikel 17*bis* van de wet van 8 december 1992, aangesteld binnen iedere inlichtingen- en veiligheidsdienst.

Hij valt onder het rechtstreekse gezag van het diensthoofd aan wie hij uitsluitend rekenschap aflegt en verslag uitbrengt. Hij is op onafhankelijke wijze belast met :

— het waarborgen van de naleving van de wet bij iedere vraag om gegevens;

— het nemen van alle nuttige maatregelen teneinde de veiligheid van de geregistreerde informatie te verzekeren;

— het verstrekken van passende adviezen aan het diensthoofd;

— het uitvoeren van andere opdrachten die hem door het diensthoofd toevertrouwd zijn.

De raadgever informatieveiligheid en bescherming van de persoonlijke levenssfeer bedoeld in het eerste lid kan zich door één of meer adjuncten laten bijstaan.

§ 2. Wat de Veiligheid van de Staat betreft, wordt de functie van raadgever informatieveiligheid en bescherming van de persoonlijke levenssfeer, die onder meer de functie vervult van aangestelde voor de gegevensbescherming bedoeld in § 1, uitgeoefend door de raadsman voor de veiligheid van de gegevens aangesteld door de Minister van Justitie overeenkomstig 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.

CHAPITRE II. — *De l'exercice des missions de renseignement et de sécurité - De l'utilisation d'un faux nom*

Art. 2. Pour l'application de l'article 13/1, § 1er, 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 des listes des faux noms indiquant le lien avec l'agent qui les utilise.

L'agent, visé à l'alinéa 1er, enregistre, dans un journal de bord tenu à cette fin, l'utilisation du faux nom, les dates, le contexte et, le cas échéant, les incidents survenus.

CHAPITRE III. — *Des méthodes ordinaires de recueil des données Accès aux banques de données du secteur public*

Art. 3. § 1er. Pour l'application de l'article 14, alinéa 4, de la loi du 30 novembre 1998, lorsque les services de renseignement et de sécurité peuvent disposer d'un accès direct à une banque de données du secteur public contenant des données à caractère personnel, le dirigeant du service concerné tient en permanence à la disposition de la Commission de la protection de la vie privée la liste nominative des personnes habilitées à accéder à la banque de données, avec indication de leur titre et de leur fonction.

L'identité des auteurs de toute demande de consultation d'une banque de données est enregistrée dans un système de contrôle au sein du service de renseignement et de sécurité concerné. Ces informations sont conservées pendant dix ans.

§ 2. Lorsqu'un accès direct aux banques de données qui contiennent des données à caractère personnel est impossible, les informations sont communiquées immédiatement à l'agent des services de renseignement et de sécurité, sur présentation de sa carte de légitimation.

Les informations sont communiquées sous une forme compréhensible. Elles reproduisent, de manière exacte, l'ensemble des données relatives à la personne concernée.

N'est pas prise en considération la demande introduite par une personne qui ne remplit pas les formalités requises à l'alinéa 1er.

§ 3. L'accès aux banques de données, qui ne contiennent pas de données à caractère personnel, est réglé sur la base des accords conclus et selon les modalités déterminées par les autorités responsables.

Art. 4. § 1er. Un conseiller en sécurité de l'information et en protection de la vie privée, qui remplit, entre autres, la fonction de préposé à la protection des données, visé à l'article 17*bis* de la loi du 8 décembre 1992, est désigné au sein de chaque service de renseignement et de sécurité, par le ministre compétent, sur la proposition du dirigeant du service concerné.

Il est placé sous l'autorité directe du dirigeant du service auquel il rend des comptes et fait rapport exclusivement. Il est chargé de manière indépendante :

— de garantir le respect de la loi lors de toute demande de données;

— de prendre toutes mesures utiles afin d'assurer la sécurité des informations enregistrées;

— de fournir des avis qualifiés au dirigeant du service;

— d'exécuter d'autres missions qui lui sont confiées par le dirigeant du service.

Le conseiller en sécurité de l'information et en protection de la vie privée, visé à l'alinéa 1er, peut se faire assister par un ou plusieurs adjoints.

§ 2. En ce qui concerne la Sûreté de l'Etat, la fonction de conseiller en sécurité de l'information et en protection de la vie privée, qui remplit, entre autres, la fonction de préposé à la protection des données, visé au § 1er, est exercée par le conseiller à la sécurité des données désigné par le Ministre de la Justice, conformément 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.

Art. 5. De inlichtingen- en veiligheidsdiensten hebben kosteloos toegang tot de gegevensbanken van de openbare sector.

HOOFDSTUK IV. — *Specifieke methoden en uitzonderlijke methoden voor het verzamelen van gegevens*

Afdeling 1. — Fictieve identiteiten en hoedanigheden

Art. 6. Voor de toepassing van artikel 18/13, tweede lid, van de wet van 30 november 1998 houdt het betrokken diensthoofd of de persoon die hij hiertoe aanstelt, registers bij van de fictieve identiteiten en hoedanigheden en vermeldt het verband met de agent die ze gebruikt.

De agent bedoeld in het eerste lid vermeldt in een logboek dat hij hiertoe bijhoudt, het gebruik van de fictieve identiteit en/of hoedanigheid, de data, de context en, desgevallend, de incidenten die plaatsgevonden hebben. Het betrokken diensthoofd wordt hiervan regelmatig schriftelijk op de hoogte gebracht. Deze informatie wordt opgenomen in het rapport dat gericht wordt aan de commissie overeenkomstig artikel 18/13, vierde lid, van de wet van 30 november 1998.

Het logboek bedoeld in het tweede lid wordt nog tien jaar bewaard, nadat de fictieve identiteit of hoedanigheid niet meer actief is.

Afdeling 2. — Nadere regels voor de vernietiging van de opnamen en van de eventuele overschrijvingen en vertalingen van de communicaties

Art. 7. Voor de toepassing van artikel 18/17, § 7, van de wet van 30 november 1998 en onverminderd de regels betreffende de vernietiging van geclassificeerde documenten overeenkomstig de wet van 11 december 1998, gebeurt de vernietiging van de opnamen en van de eventuele overschrijvingen en vertalingen van de communicaties, naargelang de drager, door middel van de meest passende technische methodes, rekening houdend met de evolutie van de technologie ter zake, zodat ze onmogelijk nog geëxploiteerd kunnen worden.

Afdeling 3. — Vergoeding voor de medewerking van natuurlijke personen en rechtspersonen

Art. 8. Voor de toepassing van artikel 18/18 van de wet van 30 november 1998 worden de tarieven die de medewerking van de natuurlijke persoon of de rechtspersoon vergoeden, bepaald op grond van de bestaande regelgevende bepalingen inzake de gerechtskosten in strafzaken.

Bij ontstentenis van bestaande tarieven in deze bepalingen wordt het tarief van de door natuurlijke personen uitgevoerde prestaties bepaald op grond van een factuur of een onkostennota die rekening houdt met de werkelijke kost veroorzaakt door de geleverde prestatie. De tarieven die de medewerking van de rechtspersonen vergoeden, worden bepaald in functie van de eventuele meerkost die deze medewerking meebrengt in verhouding tot hun normale werking.

De natuurlijke persoon of de rechtspersoon richt het naar behoren verantwoorde en gecontroleerde detail van de uitgevoerde prestatie of van de meerkost aan het betrokken diensthoofd.

HOOFDSTUK V. — *Toezicht op de specifieke en uitzonderlijke methoden*

Afdeling 1. — Nadere regels en termijnen voor de kennisgeving van de commissie

Art. 9. Voor de toepassing van artikel 18/10, § 1, derde lid, van de wet van 30 november 1998 informeert het betrokken diensthoofd de commissie om de twee weken, vanaf de dag waarop de uitzonderlijke methode toegepast wordt, over het verloop ervan, onder voorbehoud van artikel 18/13, vierde lid, van dezelfde wet. Het diensthoofd informeert de commissie ook wanneer de methode beëindigd is.

Onverminderd de regels en richtlijnen betreffende de overdracht van geclassificeerde informatie krachtens de wet van 11 december 1998, brengt het betrokken diensthoofd de commissie op de hoogte via beveiligde elektronische weg of, indien dit onmogelijk is, per drager.

Art. 10. In de gevallen van uiterste hoogdringendheid bedoeld in artikel 18/10, § 4, eerste lid, van de wet van 30 november 1998, deelt het betrokken diensthoofd onmiddellijk via beveiligde elektronische weg of, indien dat onmogelijk is, per drager, zijn machtiging mee aan de leden van de commissie.

Het eerste lid doet geen afbreuk aan de regels en richtlijnen betreffende de overdracht van geclassificeerde informatie krachtens de wet van 11 december 1998.

Afdeling 2. — Nadere regels voor de kennisgevingen zoals bedoeld in artikel 43/3 van de wet van 30 november 1998

Art. 11. Voor de toepassing van artikel 43/3, eerste lid, van de wet van 30 november 1998, worden de lijsten bedoeld in artikel 18/3, § 2, van de wet van 30 november 1998, door de commissie meegedeeld aan het Vast Comité I zodra zij deze heeft ontvangen.

Art. 5. Les services de renseignement et de sécurité accèdent sans frais aux banques de données du secteur public.

CHAPITRE IV. — *Des méthodes spécifiques et des méthodes exceptionnelles de recueil des données*

Section 1re. — Des identités et qualités fictives

Art. 6. Pour l'application de l'article 18/13, alinéa 2, de la loi du 30 novembre 1998, le dirigeant du service concerné ou la personne qu'il désigne à cet effet tient des registres des identités et qualités fictives indiquant le lien avec l'agent qui les utilise.

L'agent, visé à l'alinéa 1er, indique dans un journal de bord, tenu par lui à cet effet, l'utilisation de l'identité et/ou de la qualité fictive, les dates, le contexte et, le cas échéant, les incidents survenus. Le dirigeant du service concerné en est informé régulièrement par écrit. Cette information est intégrée dans le rapport adressé à la commission, conformément à l'article 18/13, alinéa 4, de la loi du 30 novembre 1998.

Le journal de bord, visé à l'alinéa 2, est conservé pendant dix ans après que l'identité ou la qualité fictive ne soit plus active.

Section 2. — Des modalités de destruction des enregistrements, transcriptions et traductions éventuelles des communications

Art. 7. Pour l'application de l'article 18/17, § 7, de la loi du 30 novembre 1998, sans préjudice des règles relatives à la destruction des documents classifiés conformément à la loi du 11 décembre 1998, la destruction des enregistrements, transcriptions et traductions éventuelles des communications est effectuée, selon le support, au moyen des procédés techniques les plus appropriés, compte tenu de l'évolution de la technologie en la matière, de sorte qu'il ne soit plus possible de les exploiter.

Section 3. — De la rétribution de la collaboration des personnes physiques et des personnes morales

Art. 8. Pour l'application de l'article 18/18 de la loi du 30 novembre 1998, les tarifs rétribuant la collaboration de la personne physique ou de la personne morale sont déterminés sur la base des dispositions règlementaires existantes sur les frais de justice en matière répressive.

A défaut de tarifs existants dans ces dispositions, le tarif des prestations effectuées par les personnes physiques est déterminé sur la base d'une facture ou d'une note de frais qui tient compte du coût réellement supporté en raison de l'exécution de la prestation. Les tarifs rétribuant la collaboration des personnes morales sont déterminés en fonction du surcoût éventuel que cette collaboration engendre par rapport à leur fonctionnement normal.

La personne physique ou la personne morale adresse au dirigeant du service concerné, en fonction de la nature de l'intervention, le détail de la prestation effectuée ou du surcoût, dûment justifié et contrôlé.

CHAPITRE V. — *Du contrôle des méthodes spécifiques et exceptionnelles*

Section 1re. — Des modalités et délais d'information de la commission

Art. 9. Pour l'application de l'article 18/10, § 1er, alinéa 3, de la loi du 30 novembre 1998, le dirigeant du service concerné informe la commission du déroulement de l'exécution de la méthode exceptionnelle toutes les deux semaines, à partir du jour où elle est mise en œuvre, sous réserve de l'article 18/13, alinéa 4, de la même loi, et lorsqu'elle prend fin.

Sans préjudice des règles et directives relatives à la transmission d'informations classifiées en vertu de la loi du 11 décembre 1998, le dirigeant du service concerné informe la commission par voie électronique sécurisée ou, en cas d'impossibilité, par porteur.

Art. 10. Dans les cas d'extrême urgence, visés à l'article 18/10, § 4, alinéa 1er, de la loi du 30 novembre 1998, le dirigeant du service concerné communique immédiatement son autorisation aux membres de la commission, par voie électronique sécurisée ou, en cas d'impossibilité, par porteur.

L'alinéa 1er ne porte pas préjudice aux règles et directives relatives à la transmission d'informations classifiées en vertu de la loi du 11 décembre 1998.

Section 2. — Modalités pour les communications telles que visées à l'article 43/3 de la loi du 30 novembre 1998

Art. 11. Pour l'application de l'article 43/3, alinéa 1er, de la loi du 30 novembre 1998, les listes, visées à l'article 18/3, § 2, de la loi du 30 novembre 1998, sont communiquées au Comité permanent R par la commission, dès réception de celles-ci.

Voor de toepassing van artikel 43/3, tweede lid, van de wet van 30 november 1998, wordt elke beslissing om een specifieke methode toe te passen, elke machtiging om een uitzonderlijke methode toe te passen, te beëindigen, te schorsen, elke beslissing houdende het verbod om onwettelijk verkregen gegevens te exploiteren en elk advies of elke machtiging omtrent deze methoden, onverwijld en integraal door de commissie ter kennis gebracht van het Vast Comité I.

De kennisgevingen bedoeld in het eerste en tweede lid gebeuren 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.

Naar aanleiding van de kennisgeving bedoeld in het vorige lid wordt voor elke afzonderlijke beslissing, advies of machtiging, naargelang het geval, op gestructureerde wijze de volgende gegevens meegedeeld :

— de identiteit van de overheid die de beslissing genomen heeft of het advies of de machtiging verleend heeft;

— de datum van de beslissing, het advies of de machtiging;

— de aard van de specifieke of uitzonderlijke methode voor het verzamelen van gegevens;

— de aard van de dreiging en van het te vrijwaren belang;

— de graad van de ernst van de bedreiging;

— de beoordeling van de proportionaliteit en van de subsidiariteit;

— de natuurlijke perso(o)n(en) of rechtsperso(o)n(en), verenigingen of groeperingen, voorwerpen, plaatsen, gebeurtenissen of informatie die het onderwerp zijn van de methode;

— de hoedanigheid van advocaat, arts of journalist van de perso(o)n(en) die het onderwerp zijn van de methode;

— het feit dat door een advocaat, een arts of een journalist lokalen aangewend worden voor beroepsdoeleinden of als woonplaats;

— het technische middel dat gebruikt wordt om de methode aan te wenden;

— de periode tijdens welke de methode kan worden uitgevoerd, te rekenen vanaf de kennisgeving van de beslissing of de machtiging;

— het feit of de beslissing, de machtiging of het advies betrekking heeft op een verlenging.

Het Vast Comité I geeft ontvangstmelding van elke kennisgeving.

De kennisgevingen geschieden met inachtneming van de regels en richtlijnen betreffende de overdracht van geclassificeerde informatie krachtens de wet van 11 december 1998.

Afdeling 3. — Nadere regels en termijnen voor de bewaring van gegevens die onwettig verzameld zijn door een specifieke of uitzonderlijke methode

Art. 12. Voor de toepassing van de artikelen 18/3, § 2, vierde lid, en 18/10, § 6, vierde lid, van de wet van 30 november 1998, worden de gegevens die verzameld zijn in omstandigheden die de geldende wettelijke bepalingen niet naleven, met het oog op hun bewaring, onverwijld in een verzegelde omslag geplaatst op een beveiligde plaats die door de commissie bepaald wordt in overleg met het betrokken diensthoofd, overeenkomstig de regels en richtlijnen betreffende de bewaring van de krachtens de wet van 11 december 1998 geclassificeerde gegevens.

Als de gegevens, bedoeld in het eerste lid, geïnformatiseerd zijn, worden zij, in afwachting van de beslissing van het Vast Comité I, bedoeld in artikel 43/6, § 1, van de wet van 30 november 1998, tijdelijk ontoegankelijk gemaakt, behalve voor de raadgever informatieveiligheid en bescherming van de persoonlijke levenssfeer, door middel van de meest passende technische methoden rekening houdende met de evolutie van de technologie ter zake, zodat ze onmogelijk nog door de inlichtingen- en veiligheidsdiensten geëxploiteerd kunnen worden.

Afdeling 4. — Nadere regels voor de vernietiging van gegevens die onwettig verzameld zijn door een specifieke of uitzonderlijke methode

Art. 13. Voor de toepassing van artikel 43/6, § 1, eerste lid, van de wet van 30 november 1998, indien het Vast Comité I beslist dat de gegevens verzameld werden in omstandigheden die de geldende wettelijke bepalingen niet naleven, worden de gegevens zo snel mogelijk vernietigd en ten laatste een maand na de mededeling van de beslissing aan het betrokken diensthoofd.

Pour l'application de l'article 43/3, alinéa 2, de la loi du 30 novembre 1998, toute décision de mettre en oeuvre une méthode spécifique ou toute autorisation de mettre en oeuvre une méthode exceptionnelle, d'y mettre fin, de la suspendre, toute décision interdisant l'exploitation de données recueillies illégalement et tout avis ou toute autorisation en rapport avec ces méthodes est intégralement communiqué(e) au Comité permanent R par la commission.

Les communications visées aux alinéas 1er et 2 se font 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.

A l'occasion de la communication visée au précédent alinéa, pour toute décision, avis ou autorisation particuliers, les données suivantes sont, selon le cas, communiquées de manière structurée :

— l'identité de l'autorité qui a pris la décision ou a donné l'avis ou l'autorisation;

— la date de la décision, de l'avis ou de l'autorisation;

— la nature de la méthode spécifique ou exceptionnelle pour le recueil de données;

— la nature de la menace et de l'intérêt à préserver;

— le degré de gravité de la menace;

— l'évaluation de la proportionnalité et de la subsidiarité;

— le(s) personne(s) physique(s) ou morale(s), associations ou groupements, matériels, lieux, évènements ou informations qui sont soumis à la méthode;

— la qualité d'avocat, de médecin ou de journaliste de la/les personne(s) soumise(s) à la méthode;

— le fait que des locaux soient utilisés par un avocat, un médecin ou un journaliste à des fins professionnelles ou comme résidence;

— le moyen technique qui est employé pour la mise en œuvre de la méthode;

— la période au cours de laquelle la méthode peut être mise en œuvre, à compter de la notification de la décision ou à compter de l'autorisation;

— le fait que la décision, l'autorisation ou l'avis concerne une prolongation.

Le Comité permanent R accuse réception de toute communication.

Les communications s'effectuent dans le respect des règles et directives concernant le transfert d'informations classifiées en vertu de la loi du 11 décembre 1998.

Section 3. — Des modalités et délais de conservation des données illégalement recueillies par une méthode spécifique ou exceptionnelle

Art. 12. Pour l'application des articles 18/3, § 2, alinéa 4, et 18/10, § 6, alinéa 4, de la loi du 30 novembre 1998, les données recueillies dans des conditions qui ne respectent pas les dispositions légales en vigueur sont placées sous scellé, sans délai, en vue de leur conservation, dans un lieu sécurisé désigné par la commission, en concertation avec le dirigeant du service concerné, conformément aux règles et directives relatives à la conservation des données classifiées en vertu de la loi du 11 décembre 1998.

Si les données, visées à l'alinéa 1er, sont informatisées, elles sont rendues temporairement inaccessibles, sauf pour le conseiller en sécurité de l'information et en protection de la vie privée, dans l'attente de la décision du Comité permanent R, visée à l'article 43/6, § 1er, de la loi du 30 novembre 1998, au moyen des procédés techniques les plus appropriés, compte tenu de l'évolution de la technologie en la matière, de sorte qu'il ne soit pas possible pour les services de renseignement et de sécurité de les exploiter.

Section 4. — Des modalités de destruction des données illégalement recueillies par une méthode spécifique ou exceptionnelle

Art. 13. Pour l'application de l'article 43/6, § 1er, alinéa 1er, de la loi du 30 novembre 1998, lorsque le Comité permanent R décide que les données ont été recueillies dans des conditions qui ne respectent pas les dispositions légales en vigueur, celles-ci sont détruites dans les plus brefs délais et, au plus tard, un mois après la communication de sa décision au dirigeant du service concerné.

Het betrokken diensthoofd informeert onverwijld de overheden waaraan de gegevens meegedeeld werden, over hun onwettigheid en hun vernietiging.

Ten laatste drie werkdagen vóór de vernietiging stelt het betrokken diensthoofd de commissie schriftelijk op de hoogte van de voorziene datum. De vernietiging wordt uitgevoerd onder het toezicht van een lid van de commissie en van het betrokken diensthoofd of de persoon die hij hiertoe aanstelt.

Onverminderd de regels betreffende de vernietiging van geclassificeerde documenten overeenkomstig de wet van 11 december 1998, wordt de vernietiging van de gegevens bedoeld in het eerste lid, naargelang de drager, uitgevoerd door middel van de meest passende technische methoden, rekening houdend met de evolutie van de technologie ter zake, zodat zij onmogelijk nog geëxploiteerd kunnen worden.

De persoon die de vernietiging uitvoert stelt een vernietigingsrapport op dat wordt medeondertekend door de personen bedoeld in het derde lid, alsook door een veiligheidsofficier van de betrokken dienst. Het rapport wordt bewaard binnen deze dienst. Een kopie van het rapport wordt aan het Vast Comité I gericht.

HOOFDSTUK VI. — *Adiëring van het Vast Comité I door de Commissie voor de bescherming van de persoonlijke levenssfeer op grond van artikel 43/4 van de wet van 30 november 1998*

Art. 14. Indien 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 een redelijk vermoeden heeft dat persoonsgegevens in de zin van deze wet, die door een inlichtingen- en veiligheidsdienst worden verwerkt, zijn verzameld via een specifieke of uitzonderlijke methode maar met miskenning van de regels vervat in de wet van 30 november 1998, kan ze een met redenen omkleed verzoek tot het Vast Comité I richten.

Het verzoek bevat minstens volgende elementen :

— de betrokken inlichtingen- en veiligheidsdienst;

— een aanduiding van de bedoelde persoonsgegevens;

— de elementen die de Commissie voor de bescherming van de persoonlijke levenssfeer doen vermoeden dat deze gegevens via een specifieke of uitzonderlijke methode werden verzameld;

— de elementen die de Commissie voor de bescherming van de persoonlijke levenssfeer doen vermoeden dat deze gegevens met miskenning van de regels vervat in de wet van 30 november 1998 werden verzameld.

Het verzoek wordt aan het Vast Comité I overgezonden bij aangetekend schrijven of op elke andere in onderling overleg overeengekomen wijze. In beide gevallen worden de regels en richtlijnen betreffende de overdracht van geclassificeerde informatie krachtens de wet van 11 december 1998 nageleefd.

HOOFDSTUK VII. — *Eindbepalingen*

Art. 15. Onze Minister van Justitie en Onze Minister van Landsverdediging zijn ieder wat hem betreft, belast met de uitvoering van dit besluit.

Art. 16. Dit besluit treedt in werking de dag waarop het in het *Belgisch Staatsblad* wordt bekendgemaakt.

Gegeven te Brussel, 12 oktober 2010.

ALBERT

Van Koningswege :

De Minister van Justitie,
S. DE CLERCK

De Minister van Landsverdediging,
P. DE CREM

Le dirigeant du service concerné avertit, sans délai, les autorités auxquelles les données ont été communiquées de leur illégalité et de leur destruction.

Au plus tard trois jours ouvrables avant la destruction, le dirigeant du service concerné informe, par écrit, la commission de la date prévue. La destruction est opérée sous le contrôle d'un membre de la commission et du dirigeant du service concerné ou de la personne qu'il désigne à cet effet.

Sans préjudice des règles relatives à la destruction des documents classifiés conformément à la loi du 11 décembre 1998, la destruction des données, visées à l'alinéa 1er, est effectuée, selon le support, au moyen des procédés techniques les plus appropriés, compte tenu de l'évolution de la technologie en la matière, de sorte qu'il ne soit plus possible de les exploiter.

Un rapport de destruction est rédigé par l'auteur de la destruction et est contresigné par les personnes, visées à l'alinéa 3, ainsi que par un officier de sécurité du service concerné. Le rapport est conservé au sein de ce service. Une copie en est adressée au Comité permanent R.

CHAPITRE VI. — *La saisine du Comité permanent R par la Commission de la protection de la vie privée en vertu de l'article 43/4 de la loi du 30 novembre 1998*

Art. 14. Si, à la suite d'une vérification sur la base de l'article 13 de la loi du 8 décembre 1992, la Commission de la protection de la vie privée a une suspicion raisonnable que des données à caractère personnel, au sens de cette loi, qui sont traitées par un service de renseignement et de sécurité, sont recueillies via une méthode spécifique ou exceptionnelle, mais au mépris des règles contenues dans la loi du 30 novembre 1998, elle peut adresser une demande motivée au Comité permanent R.

La demande reprend au moins les éléments suivants :

— le service de renseignement et de sécurité concerné;

— une indication des données à caractère personnel visées;

— les éléments ayant fait naître la suspicion de la Commission de la protection de la vie privée que ces données ont été recueillies via une méthode spécifique ou exceptionnelle;

— les éléments ayant fait naître la suspicion de la Commission de la protection de la vie privée que ces données ont été recueillies au mépris des règles contenues dans la loi du 30 novembre 1998.

La demande est transmise au Comité permanent R par courrier recommandé ou de toute autre manière déterminée de commun accord. Dans les deux cas, les règles et directives concernant la transmission d'informations classifiées en vertu de la loi du 11 décembre 1998 sont respectées.

CHAPITRE VII. — *Dispositions finales*

Art. 15. Le Ministre de la Justice et le Ministre de la Défense chacun en ce qui les concerne, sont chargés de l'exécution du présent arrêté.

Art. 16. Le présent arrêté entre en vigueur le jour de sa publication au *Moniteur belge.*

Donné à Bruxelles, le 12 octobre 2010.

ALBERT

Par le Roi :

Le Ministre de la Justice,
S. DE CLERCK

Le Ministre de la Défense,
P. DE CREM