**ADVIES 002/VCI-BTA/2019 VAN 9 APRIL 2019**
**Wijziging KB 12 oktober 2010 en KB 3 juli 2016**

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

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

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

**AVIS 002/CPR-ACC/2019 DU 9 AVRIL 2019**
**Modification de l'A.R. du 12 octobre 2010 et de l'A.R. du 3 juillet 2016**

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

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

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

Vast Comité I – moet inwinnen.

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

- de Wet van 30 maart 2017 die talrijke wijzigingen aanbracht aan de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (W.I&V);
- de Wet van 21 maart 2018 tot wijziging van de Wet op het politieambt om het gebruik van camera's door de politiediensten te regelen, en tot wijziging van de Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's, van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en van de Wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid waarbij artikel 16/4 in de W.I&V werd ingevoegd om inlichtingendiensten toe te laten toegang te hebben tot informatie en persoonsgegevens die verzameld worden door middel van door de politiediensten gebruikte camera's.

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

l'occurrence le Comité permanent R.

2. Le projet d'arrêté proposé donne exécution à trois lois :
- la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD), qui a désigné le Comité permanent R comme autorité de protection des données pour le traitement des données à caractère personnel par les services de renseignement et qui a introduit quelques autres dispositions. Celles-ci impliquent des adaptations, d'une part de l'Arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité et, d'autre part, de l'Arrêté royal du 3 juillet 2016 portant exécution de l'article 21 de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité' ;
- la Loi du 30 mars 2017 qui apporte de nombreuses modifications à la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S) ;
- la Loi du 21 mars 2018 modifiant la Loi sur la fonction de police en vue de régler l'utilisation de caméras par les services de police, et modifiant la Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la Loi du 2 octobre 2017 réglementant la sécurité privée et particulière qui a inséré l'article 16/4 dans la L.R&S, permettant aux services de renseignement d'avoir accès aux informations et données à caractère personnel qui sont collectées au moyen de caméras utilisées par les services de police.

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

***Bewaringstermijn voor de logboeken en het arrestatieregister***

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

Het Comité ziet niet in waarom deze gegevens – die overigens nauwelijks opslagcapaciteit vereisen – in theorie reeds na vijf jaar zouden kunnen vernietigd worden. Dergelijke vernietiging maakt elke latere controle door het Comité onmogelijk. Het Comité wijst er op dat het KB van 12 oktober 2010 reeds voorziet in een bewaartermijn van tien jaar voor de logs in de gegevensbanken van de openbare sector (art. 3 § 1) of voor de logboeken waarin de fictieve identiteit of hoedanigheid is opgenomen van agenten die opereren binnen fictieve rechtspersonen (art. 6). Het Comité wijst er ten slotte op dat het hanteren van een valse naam of hoedanigheid of de arrestatie van een persoon buiten het wettelijk kader een misdrijf kan uitmaken en dat het logboek/register in dat verband zou kunnen gehanteerd worden als bewijselement en dit zowel *à charge* als *à décharge*. Ook vanuit dit perspectief zou een vernietiging na vijf jaar voor onnodige moeilijkheden kunnen zorgen. Ten slotte is het mogelijk dat deze logs relevant blijken in andere strafonderzoeken waaraan de inlichtingendiensten bijvoorbeeld hun technische bijstand hebben verleend of waarbij zij informatie hebben verschaft.

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

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

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

Le Comité ne voit pas pourquoi ces données – qui nécessitent d'ailleurs peu de capacités de stockage – devraient déjà être théoriquement détruites après cinq ans. Une telle destruction rend impossible tout contrôle ultérieur par le Comité, qui fait remarquer que l'A.R. du 12 octobre 2010 prévoit déjà un délai de conservation de dix ans pour les logs dans les banques de données du secteur public (art. 3 §1er) ou pour les journaux de bord reprenant l'identité ou la qualité fictive d'agents qui opèrent au sein de personnes morales fictives (art. 6). Enfin, le Comité attire l'attention sur le fait que l'utilisation d'un faux nom ou d'une fausse qualité, ou encore l'arrestation d'une personne en dehors du cadre légal, peut constituer une infraction, et que le journal de bord/registre à cet égard pourrait être utilisé comme un élément de preuve tant à charge qu'à décharge. Dans cette perspective aussi, une destruction après cinq ans pourrait donner lieu à des complications inutiles. Enfin, il est possible que ces logs se révèlent être pertinents dans d'autres enquêtes pénales auxquelles les services de renseignement ont, par exemple, prêté leur assistance technique ou pour lesquelles ils ont fourni des informations.

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

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

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

***Toegang tot gegevensbanken van de openbare en private sector***

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

- *'Deze wijziging van het koninklijk besluit verleent geen toegang tot een externe gegevensbank, het bepaalt enkel de nadere regels die moeten worden toegepast wanneer een dergelijke toegang bestaat door of krachtens een wet of met de toestemming van de verwerkingsverantwoordelijke van de gegevensbank.';*
- *'Artikel 6 wijzigt artikel 3 van het koninklijk besluit van 12 oktober 2010 om de toegangsbepalingen vast te leggen voor elke gegevensbank waartoe de inlichtingen- en veiligheidsdiensten toegang hebben of zullen hebben, door of krachtens een specifieke wet, of,*

matière pénale.

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

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

***Accès aux banques de données des secteurs public et privé***

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

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

- *'L'article 6 adapte l'article 3 de l'arrêté royal du 12 octobre 2010 afin de fixer les modalités d'accès à toute banque de données auxquelles les services de renseignement ont ou auront accès, par ou en vertu d'une loi spécifique ou, sur base des*

*op basis van artikelen 14 (gegevens van het openbare sector) of 16 (gegevens van het private sector), met de toestemming van de verwerkingsverantwoordelijke van de gegevensbank.'*
*- 'Dit artikel voert meer bepaald de artikelen 14, 16/2 en 16/4 van de wet van 30 november 1998 uit.'*
Het Vast Comité I noteert dan ook dat de in het ontwerpbesluit vastgestelde regels dus gelden voor databanken van publieke én private (rechts)personen en dit zowel voor databanken waartoe een inlichtingendienst reeds toegang heeft (door of krachtens een wet of met toestemming van de verwerkingsverantwoordelijke) of in de toekomst toegang zal krijgen.

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

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

*articles 14 (données du secteur public) et 16 (données du secteur privé) de la loi organique, avec le consentement du responsable du traitement de la banque de données'.*
*- 'Cet article exécute notamment les articles 14, 16/2 et 16/4 de la loi du 30 novembre 1998'.*
Le Comité permanent R note dès lors que les règles fixées dans le projet d'arrêté valent pour les banques de données de personnes (morales) publiques et privées, et ce tant pour les banques de données auxquelles un service de renseignement a déjà accès (par ou en vertu d'une loi ou avec l'accord des responsables du traitement) que pour banques de données auxquelles il aura accès dans le futur.

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

8. En ce qui concerne l'accès octroyé par ou en vertu de la loi aux fichiers qui sont conservés par des personnes (morales) privées, citons, par exemple, l'article 16/2 L.R&S qui dispose que l'on peut procéder à l'identification de personnes qui utilisent un moyen de communication déterminé non seulement par le biais d'une réquisition à l'opérateur ou au fournisseur de services, mais aussi *'au moyen d'un accès aux fichiers*

*van de principes van proportionaliteit en subsidiariteit en mits de registratie van de raadpleging'* en dit onder de door de Koning bepaalde *'technische voorwaarden'*.

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

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

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

Het Vast Comité I benadrukt opnieuw dat de mogelijkheid om rechtstreeks toegang te krijgen tot gegevensbanken niet mag gebruikt worden om wettelijke procedures die in een specifieke

*des clients'*, *'dans le respect des principes de proportionnalité et de subsidiarité, et moyennant l'enregistrement de la consultation'*, et ce dans les *'conditions techniques'* fixées par le Roi.

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

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

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

Le Comité permanent R souligne à nouveau que la possibilité d'obtenir un accès direct à des banques de données ne peut être utilisée pour contourner des procédures

controle voorzien, te omzeilen. Bedoeld wordt bijvoorbeeld de rechtstreekse toegang tot lokalisatiegegevens bijgehouden door telecombedrijven of financiële gegevens verwerkt door bankinstellingen terwijl dit een specifieke of uitzonderlijke methode vormt. In deze gevallen mag geen rechtstreekse toegang of bevraging worden georganiseerd.

10. Indien bij of krachtens de wet of na akkoord van de verwerkingsverantwoordelijke een rechtstreekse toegang mogelijk wordt gemaakt, zullen minstens (in de wet, het krachtens de wet genomen besluit of het akkoord kunnen bijkomende regels geformuleerd worden) een aantal regels moeten gerespecteerd worden. Deze regels werden opgenomen in het ontwerpbesluit. Vooraf dient evenwel benadrukt dat het ontwerpbesluit niet alleen de modaliteiten voor een *'rechtstreekse toegang'* maar ook voor een *'rechtstreekse bevraging'* regelt. Het ontwerp preciseert echter niet wat hieronder dient te worden begrepen. Het Comité beveelt aan dat het KB deze termen nader definieert. Daarbij kan best aansluiting gezocht worden bij de definitie zoals opgenomen in artikel 44/11/4 van de Wet op het Politieambt. *'Onder 'rechtstreekse toegang' wordt een geautomatiseerde verbinding [...] verstaan die het mogelijk maakt toegang te hebben tot de [in de databank] vervatte gegevens.'* en *'Onder 'rechtstreekse bevraging' wordt een beperkte rechtstreekse toegang tot alle of een gedeelte van de volgende gegevens verstaan: a) het bestaan van gegevens over een persoon met toepassing van de artikelen 44/5, § 1, eerste lid, 2° tot 6°, en § 3, 1° tot 9°; b) de door de politie weerhouden kwalificatie betreffende de feiten waarvoor de persoon geregistreerd werd; c) de noodzakelijke gegevens om meer informatie te bekomen vanwege de bevoegde overheid; d) de gegevens met betrekking tot de te nemen maatregelen voor de in punt a) bedoelde personen.'*

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

légales qui prévoient un contrôle spécifique. On entend par là, par exemple, l'accès direct à des données de localisation conservées par des entreprises de télécommunication ou des données financières traitées par des institutions bancaires, alors qu'il s'agit d'une méthode spécifique ou exceptionnelle. Dans ces cas-là, aucun accès ni interrogation direct(e) ne peut être organisé(e).

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

*a) l'existence de données sur une personne en application de l'article 44/5, § 1er, alinéa 1er, 2° à 6°, et § 3, 1° à 9° ;*

*b) la qualification retenue par la police concernant les faits pour lesquels la personne est enregistrée;*

*c) les données nécessaires pour obtenir plus d'informations auprès de l'autorité compétente;*

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

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

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

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

14. In het voorgestelde tweede lid wordt bepaald dat de rechtstreekse toegang ook kan *'gerealiseerd worden door het verschaffen van persoonsgegevensbestanden'*. In het Verslag aan de Koning wordt hierover het volgende gesteld: *'Ter illustratie: de DIV geeft veeleer de voorkeur aan de mededeling van bestanden aan een ontvanger dan aan een raadpleging van zijn gegevensbank om te voorkomen dat de verwerkingen van zijn eigen diensten in de gegevensbank traag verlopen door een overbelasting van het systeem'*. Het Comité wijst er op dat het op dat ogenblik niet meer over een rechtstreekse toegang of bevraging gaat maar over een gewone vraag tot informatie zoals bepaald in artikel 14, tweede en derde lid en artikel 16, tweede lid W.I&V. Het Comité ziet overigens niet in hoe het antwoord op dergelijke vragen de opslagcapaciteit van een inlichtingendienst te boven kan gaan, tenzij de vraag betrekking zou hebben op de gehele of grote delen van een databank. In dat geval stellen zich uiteraard andere principiële vragen bij de voorgestelde tekst, zoals bijvoorbeeld de vraag naar proportionaliteit en finaliteit. Tevens zou de betrokken inlichtingendienst in dat geval beschikken over een 'kopie' van een databank waarvan de gegevens na verloop van tijd onvermijdelijk gedateerd en dus niet accuraat zijn. Het Comité acht om al die redenen een

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

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

14. Dans le deuxième alinéa proposé, il est précisé que l'accès direct peut également être 'réalisé par la fourniture de fichiers de données à caractère personnel'. Le Rapport au Roi reprend à cet égard les termes suivants : 'A titre d'illustration, la DIV préfère la communication de fichiers vers un destinataire plutôt qu'une consultation dans sa banque de données, afin d'éviter une lenteur des traitements de ses propres services dans la banque de données, due à une surcharge du système'. Le Comité fait remarquer qu'à ce moment-là, il ne s'agit plus d'un accès ou d'une interrogation direct(e), mais d'une simple demande d'information, telle que prévue à l'article 14, alinéas 2 et 3 et à l'article 16, alinéa 2 L.R&S. Le Comité ne comprend d'ailleurs pas comment la réponse à de telles questions peut excéder la capacité de stockage d'un service de renseignement, à moins que la question ne porte sur l'ensemble ou sur de larges pans d'une banque de données. Dans ce cas, se posent évidemment d'autres questions de principe sur le texte proposé, comme par exemple la question de la proportionnalité et de la finalité. Dans ce cas, le service de renseignement concerné disposerait aussi d'une 'copie' d'une base de données dont les données ne seraient plus à

vorm van 'kopiename' niet conform de basisprincipes van dataprotectie.

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

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

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

Artikel 13 Gegevensbeschermingswet luidt als volgt:
*'Wanneer een overheid bedoeld in ondertitels 1* [zijnde de inlichtingendiensten, nvda] *en 6 van titel 3 over een rechtstreekse toegang of over een rechtstreekse bevraging van een gegevensbank van de openbare of private sector beschikt, worden zijn verwerkingen van persoonsgegevens in deze gegevensbank beschermd door technische, organisatorische en individuele beveiligingsmaatregelen zodat alleen de volgende actoren toegang kunnen hebben tot de*

jour, inévitablement, et seraient donc inexactes. Pour toutes ces raisons, le Comité considère qu'une forme de 'copie' n'est pas conforme aux principes fondamentaux de la protection des données.

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

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

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

L'article 13 de la Loi protection des données est libellé comme suit :
*'Lorsqu'une autorité visée aux sous-titres 1er* [c'est-à-dire les services de renseignement, ndr] *et 6 du titre 3 dispose d'un accès direct ou d'une interrogation directe à une banque de données du secteur public ou du secteur privé, ses traitements de données à caractère personnel dans cette banque de données sont protégés par des mesures de sécurité techniques, organisationnelles et individuelles de sorte que seuls les acteurs*

*inhoud van deze verwerkingen om hun wettelijke toezichtsopdrachten uit te voeren:*

*1° de functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke van de gegevensbank;*
*2° de functionaris voor gegevensbescherming van de overheid bedoeld in de ondertitels 1 en 6 van titel 3;*
*3° de verwerkingsverantwoordelijke van de gegevensbank of zijn gemachtigde;*
*4° de verwerkingsverantwoordelijke van de overheid bedoeld in de ondertitels 1 en 6 van titel 3;*
*5° elke andere persoon bepaald in een protocol tussen de verwerkingsverantwoordelijken voor zover de toegang past in de uitvoering van de wettelijke toezichtsopdrachten van de functionarissen voor gegevensbescherming en de verwerkingsverantwoordelijken.*
*De in het eerste lid vermelde beveiligingsmaatregelen zijn bedoeld om de wettelijke verplichtingen met betrekking tot de bescherming van bronnen, de bescherming van de identiteit van de agenten of de discretie van de onderzoeken van de overheden bedoeld in ondertitels 1 en 6 van titel 3 te beschermen. Zij worden ter beschikking gesteld van de bevoegde toezichthoudende autoriteit.*
*Deze verwerkingen mogen enkel toegankelijk zijn voor andere doeleinden dan deze die verband houden met het toezicht indien deze doeleinden vastgelegd zijn in een protocolakkoord door de betrokken verwerkingsverantwoordelijken binnen de doeleinden voorzien door of krachtens een wet.*
*Het protocolakkoord duidt de persoon of personen aan waarvoor de toegang tot de logbestanden noodzakelijk is ter vervulling van elke doeleinde toegelaten in het derde lid.*
*De logbestanden en de in het eerste lid vermelde beveiligingsmaatregelen worden ter beschikking gesteld van het Vast Comité I.*
*De betrokken overheid bedoeld in titel 3 kan afwijken van het eerste lid wanneer de toegang tot zijn verwerkingen in een gegevensbank en de logbestanden geen afbreuk kan doen aan de belangen bedoeld in het tweede lid'.*
Artikel 47 Gegevensbeschermingswet is volledig gelijkaardig.

*suivants puissent accéder au contenu de ces traitements pour assurer leurs missions légales de contrôle :*
*1° le délégué à la protection des données du responsable du traitement de la banque de données ;*
*2° le délégué à la protection des données de l'autorité visée aux sous-titres 1 et 6 du titre 3 ;*
*3° le responsable du traitement de la banque de données ou son délégué;*
*4° le responsable du traitement de l'autorité visée aux sous-titres 1 et 6 du titre 3 ;*

*5° toute autre personne précisée dans un protocole entre les responsables du traitement, pour autant que l'accès s'inscrive dans l'exercice des missions légales de contrôle des délégués à la protection des données et des responsables du traitement.*
*Les mesures de sécurité mentionnées à l'alinéa 1er visent à protéger les obligations légales portant sur la protection des sources, la protection de l'identité de leurs agents ou la discrétion des enquêtes des autorités visées aux sous-titres 1 et 6 du titre 3. Elles sont mises à la disposition de l'autorité de contrôle compétente.*

*Ces traitements ne peuvent être accessibles pour d'autres finalités que celles liées au contrôle que si ces finalités sont consignées dans un protocole d'accord par les responsables du traitement concernés parmi les finalités déterminées par ou en vertu de la loi.*
*Le protocole d'accord désigne la ou les personnes dont l'accès aux journaux est nécessaire pour remplir chaque finalité autorisées à l'alinéa 3.*
*Les journaux et les mesures de sécurité mentionnées à l'alinéa 1er sont mis à la disposition du Comité permanent R.*
*L'autorité visée au titre 3 concernée peut déroger à ses traitements dans une banque de données et aux journaux n'est pas susceptible de porter atteinte aux intérêts visés à l'alinéa 2.*
L'article 47 de la Loi protection des données est tout à fait similaire.

16. De voorgestelde regeling voorziet in een (beperkte) verplichting om de reden die de rechtstreekse toegang (of bevraging?) rechtvaardigen ook te loggen. De beperking bestaat erin dat dit blijkens de voorgestelde regeling alleen moet indien dit door of krachtens de wet vereist is. Het Comité is van oordeel dat dit te beperkt is: elke toegang moet een wettelijke finaliteit hebben en deze dient voorafgaand aan de consultatie vast te staan. Net zoals voor bepaalde andere gewone methoden, moet de rechtstreekse toegang afdoende gemotiveerd worden en daarbij volstaat een loutere verwijzing naar een dreiging niet. Het Comité wijst er op dat de artikelen 14 en 16 W.I&V een potentiële toegang bieden tot *quasi* alle publieke en private bestaande databanken (met uitzondering van de databanken die onder het regime van een specifieke of uitzonderlijke methode vallen) en op die wijze potentieel zeer intrusief zijn. De toegang tot de databanken is niet onderworpen aan een *a priori*-controle; er is alleen een mogelijke *ex ante*-controle door het Comité. Om deze controle effectief te maken moet de reden van elke rechtstreekse toegang, weze het op een summiere wijze, gelogd worden.

16. La réglementation proposée prévoit une obligation (limitée) de journaliser également le motif justifiant l'accès direct (ou l'interrogation ?). On entend par 'obligation limitée' qu'il convient de procéder à une journalisation, selon la réglementation proposée, uniquement si c'est requis par la loi ou en vertu de celle-ci. Trop restrictif à l'estime du Comité : tout accès doit avoir une finalité légale et celle-ci doit être définie préalablement à la consultation. Comme pour certaines autres méthodes ordinaires, l'accès direct doit être suffisamment motivé ; une simple mention de la menace ne suffit pas. Le Comité observe que les articles 14 et 16 L.R&S offrent potentiellement un accès à pratiquement toutes les banques de données existantes, qu'elles soient publiques ou privées (à l'exception des banques de données qui tombent sous le régime d'une méthode spécifique ou exceptionnelle), un tel accès pouvant se révéler très intrusif. Cet accès aux banques de données n'est pas soumis à un contrôle *a priori* ; seul un contrôle *ex ante* du Comité est possible. Pour rendre ce contrôle efficace, le motif de tout accès direct doit être journalisé, ne serait-ce que de manière sommaire.

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

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

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

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

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

***Toegang tot de ANG***

20. Het Comité merkt op dat de inlichtingendiensten tot op heden nog geen

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

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

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

***Accès à la BNG***

20. Le Comité attire l'attention sur le fait que les services de renseignement n'ont toujours

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

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

***De aanduiding van de functionaris inzake gegevensbescherming***

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

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

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

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

***La désignation du fonctionnaire en matière de protection des données***

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

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

respectievelijk gerechtelijke en administratieve politie.

***De gestructureerde mededeling van de BIM-Commissie***

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

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

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

personnel respectivement en matière de police judiciaire et de police administrative.

***La communication structurée de la Commission BIM***

22. Le projet propose de supprimer la communication structurée établie par la Commission BIM concernant chaque méthode (art. 11 alinéa 4 AR 12 octobre 2010) *'[c]es mentions ayant été reprises aux articles 18/3 et 18 /10 de la loi du 30 novembre 1998'*.
Le Comité permanent R fait néanmoins remarquer que la communication structurée reprend quelques données complémentaires qui sont pertinentes pour son contrôle : le moment où la décision de la Commission BIM est communiquée (ce n'est qu'à ce moment-là qu'une méthode spécifique peut être mise en œuvre) et le fait que la décision, l'autorisation ou l'avis porte sur une prolongation.

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

Brussel, 9 april 2019 — Bruxelles, le 9 avril 2019

VOOR ~~HET VAST COMITÉ I~~ — POUR LE COMITÉ PERMANENT R

Serge LIPSZYC
Voorzitter — Président

Wouter DE RIDDER
Griffier — Greffier