DOC 55 **2706/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

30 mai 2022

PROJET DE LOI

modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

SOMMAIRE Pages

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

30 mei 2022

WETSONTWERP

tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten

INHOUD Blz.

07058

Le gouvernement a déposé ce projet de loi le 30 mai 2022.	*De regering heeft dit wetsontwerp op 30 mei 2022 ingediend.*
Le "bon à tirer" a été reçu à la Chambre le 30 mai 2022.	*De "goedkeuring tot drukken" werd op 30 mei 2022 door de Kamer ontvangen.*

N-VA	:	*Nieuw-Vlaamse Alliantie*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
PS	:	*Parti Socialiste*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Open Vld	:	*Open Vlaamse liberalen en democraten*
Vooruit	:	*Vooruit*
Les Engagés	:	*Les Engagés*
DéFI	:	*Démocrate Fédéraliste Indépendant*
INDEP-ONAFH	:	*Indépendant - Onafhankelijk*

Abréviations dans la numérotation des publications:		*Afkorting bij de nummering van de publicaties:*	
DOC 55 0000/000	*Document de la 55e législature, suivi du numéro de base et numéro de suivi*	*DOC 55 0000/000*	*Parlementair document van de 55e zittingsperiode + basisnummer en volgnummer*
QRVA	*Questions et Réponses écrites*	*QRVA*	*Schriftelijke Vragen en Antwoorden*
CRIV	*Version provisoire du Compte Rendu Intégral*	*CRIV*	*Voorlopige versie van het Integraal Verslag*
CRABV	*Compte Rendu Analytique*	*CRABV*	*Beknopt Verslag*
CRIV	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*	*CRIV*	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénière*	*PLEN*	*Plenum*
COM	*Réunion de commission*	*COM*	*Commissievergadering*
MOT	*Motions déposées en conclusion d'interpellations (papier beige)*	*MOT*	*Moties tot besluit van interpellaties (beigekleurig papier)*

RÉSUMÉ

Le présent projet de loi prévoit principalement:

Pour les agents des services de renseignement et de sécurité:

— un élargissement des possibilités de commettre des infractions dans le cadre de leurs missions;

— la possibilité de s'infiltrer dans le monde virtuel, ou dans le monde réel;

En ce qui concerne les sources humaines:

— la possibilité pour les sources de pouvoir commettre des infractions dans le cadre de conditions strictes;

— la possibilité de pouvoir effectuer des BIM sur les sources pour contrôler leur fiabilité, leur discrétion ou leur loyauté;

Une compétence pour le Service Général du Renseignement et de la Sécurité (SGRS) est ajoutée en cas de crise nationale de cybersécurité;

Un remaniement de la méthode de collecte déjà existante auprès des institutions bancaires et financières.

Des modifications pour améliorer le travail quotidien dans la pratique ou pour réparer des oublis du législateur.

SAMENVATTING

Dit wetsontwerp regelt hoofdzakelijk:

Voor de agenten van de inlichtingen- en veiligheidsdiensten:

— een uitbreiding van de mogelijkheden om strafbare feiten te plegen in het kader van hun opdrachten;

— de mogelijkheid te infiltreren in de virtuele wereld of de reële wereld;

Voor wat betreft de menselijke bronnen:

— de mogelijkheid voor bronnen om strafbare feiten te plegen onder strikte voorwaarden;

— de mogelijkheid om BIM's uit te voeren op bronnen teneinde hun betrouwbaarheid, discretie of loyaliteit te controleren;

Er wordt een bevoegdheid voor de Algemene Dienst Inlichting en Veiligheid (ADIV) toegevoegd in geval van een nationale cybersecurity crisis;

Een herziening van de reeds bestaande methode voor het verzamelen van gegevens bij banken en financiële instellingen.

Wijzigingen om de dagelijkse werking in de praktijk te verbeteren of vergetelheden van de wetgever te corrigeren.

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

EXPOSÉ GÉNÉRAL

A titre préliminaire, le Comité permanent R (ci-après "Comité R") exprime dans son avis (point 2) que la règlementation devient trop complexe.

Les auteurs du projet réagissent le plus rapidement possible aux évolutions de la société, aux menaces qui changent et à la technologie qui se complexifie. Des changements de loi fréquents sont nécessaires.

Les auteurs n'excluent pas de restructurer la présente loi dans le futur et notamment d'unifier l'utilisation des termes, lorsqu'elle fera l'objet d'une révision globale (exemple, remplacer "commission" par "Commission",…).

Par ailleurs, en ce qui concerne les points 28, 68, 69, 76, 79, 80 de l'avis du Comité R, les auteurs du texte prennent note des remarques pertinentes et en tiendront compte lors d'une prochaine révision globale de la loi.

En réponse à l'observation générale n°1 du Conseil d'État qui demande de prévoir un mécanisme de notification active par les services de renseignement et de sécurité, les auteurs du présent texte indique qu'une proposition de loi a été déposée au Parlement et que ce dernier souhaite poursuivre ces travaux séparément.

Étant donné que les modifications envisagées sont assez techniques, il a été décidé de les discuter article par article.

COMMENTAIRE DES ARTICLES

Article 1er

L'article 1er renvoie à la répartition constitutionnelle des compétences.

MEMORIE VAN TOELICHTING

DAMES EN HEREN,

ALGEMENE TOELICHTING

Allereerst geeft het Vast Comité I (hierna "Comité I" genoemd) in zijn advies (punt 2) te kennen dat de reglementering te complex wordt.

De opstellers van het ontwerp reageren zo snel mogelijk op de ontwikkelingen van de maatschappij, op de veranderende dreigingen en op de steeds complexer wordende technologie. Frequente wetswijzigingen dringen zich dan ook op.

De opstellers sluiten niet uit deze wet in de toekomst te hervormen, met name het gebruik van de termen te uniformeren, wanneer zij het voorwerp zal uitmaken van een algemene herziening (bijvoorbeeld, "commissie" vervangen door "Commissie", …).

Daarnaast, wat de punten 28, 68, 69, 76, 79 en 80 van het advies van het Comité I betreft, nemen de auteurs van de tekst kennis van de ter zake dienende opmerkingen en zullen zij ermee rekening houden, bij een volgende algemene herziening van de wet.

In antwoord op algemene opmerking n°1 van de Raad van State, die vraagt om te voorzien in een actief kennisgevingsmechanisme door de inlichtingen- en veiligheidsdiensten, geven de opstellers van deze tekst aan dat er een wetsvoorstel werd ingediend bij het Parlement en dat dat deze laatste deze werkzaamheden afzonderlijk wenst verder te zetten.

Gezien de beoogde wijzigingen nogal technisch zijn, is ervoor gekozen om deze artikel per artikel te bespreken.

TOELICHTING BIJ DE ARTIKELEN

Artikel 1

Artikel 1 verwijst naar de grondwettelijke bevoegdheidsverdeling.

Art. 2

Le projet introduit ou adapte certaines définitions contenues à l'article 2:

"Son délégué"

L'article 2 introduit une définition à l'article 3, 8°/1 pour préciser ce que l'on vise par "son délégué", lorsque certaines décisions du dirigeant du service peuvent être prises par la personne qu'il habilite à le faire, comme c'est le cas à l'article 16/2 (identification de l'utilisateur d'un service ou moyen de communication électronique) et également à l'article 16/4 (accès aux données collectées au moyen de caméras utilisées par les services de police). La même faculté de déléguer est insérée dans l'article 16/3 dans le présent projet de loi (accès aux données PNR).

Une personne désignée pour prendre la décision ne pouvant pas être juge et partie, le gestionnaire du dossier est écarté des personnes qui peuvent être habilitées. Il est précisé, à l'instar de ce qui a été indiqué dans l'exposé des motifs de l'article 16/4 (doc 54-2855), que le terme de "gestionnaire de dossier" vise la personne qui traite un dossier ou une affaire et qui exprime le besoin de la mesure qui est soumise à l'autorisation.

Une personne désignée jouira d'une position hiérarchique supérieure à celle du gestionnaire du dossier, lorsque la structure hiérarchique du service le permet. A cet égard, la recommandation du Comité R de limiter la délégation au niveau juste inférieur au dirigeant du service adjoint ne peut pas être suivie en raison du fonctionnement des services.

La désignation doit avoir un caractère aussi permanent que possible, en fonction des moyens du service. Des changements journaliers sont exclus. Pour répondre à l'avis du Comté R (points 3 et 4), la délégation est faite par écrit par le dirigeant du service et est transmise au Comité R.

Il est évident que la désignation d'une personne habilitée à prendre certaines décisions à sa place, n'exclut pas la faculté pour le dirigeant du service de prendre lui-même ces décisions.

"L'officier des méthodes"

L'article 2 modifie également le concept d'officier de renseignement prévu à l'article 3, 9°. Suite au point 8 de l'avis du Comité R, la notion d'officier de renseignement" est remplacée par "officier des méthodes" afin de faire correspondre le titre de cet agent avec l'évolution de ses

Art. 2

Het ontwerp introduceert of wijzigt bepaalde definities in artikel 2:

"Zijn gedelegeerde"

Artikel 2 introduceert in artikel 3, 8°/1 een definitie om te preciseren wat men bedoelt onder "zijn gedelegeerde" wanneer bepaalde beslissingen van het diensthoofd mogen worden genomen door de persoon die hij hiertoe machtigt, zoals dit het geval is in artikel 16/2 (identificatie van de gebruiker van een communicatiedienst of –middel) en ook in artikel 16/4 (toegang tot de gegevens die verzameld worden door middel van camera's die door de politiediensten worden gebruikt). Deze delegatiebevoegdheid wordt in het wetsontwerp in artikel 16/3 (toegang tot de PNR-gegevens) ingevoegd.

Aangezien een persoon aangesteld om de beslissing te nemen niet rechter en partij tegelijk mag zijn, mag de dossierbeheerder hiertoe niet gemachtigd worden. Er wordt verduidelijkt, zoals vermeld in de toelichting bij artikel 16/4 (doc 54-2855), dat de term "dossierbeheerder" verwijst naar de persoon die een dossier of een zaak behandelt en daarbij de behoefte uitdrukt dat de maatregel die aan de machtiging is onderworpen, genomen wordt.

Een aangesteld persoon bekleedt een hogere hiërarchische positie dan de dossierbeheerder, wanneer de hiërarchische structuur van de dienst het toelaat. In dat opzicht kan de aanbeveling van het Comité I om de delegatie tot het niveau net onder het adjunct-diensthoofd te beperken niet worden gevolgd vanwege de werking van de diensten.

De aanstelling moet zo permanent mogelijk van aard zijn, in functie van de middelen van de dienst. Dagelijkse veranderingen zijn uitgesloten. Om te antwoorden op het advies van het Comité I (punten 3 en 4), gebeurt de delegatie schriftelijk door het diensthoofd en wordt deze overgemaakt aan het Comité I.

Het spreekt voor zich dat de aanstelling van een persoon gemachtigd om bepaalde beslissingen te nemen in zijn plaats, niet uitsluit dat het diensthoofd zelf deze beslissingen mag nemen.

"De methodenofficier"

Artikel 2 wijzigt ook het begrip van inlichtingenofficier opgenomen in artikel 3, 9°. Ingevolge het advies van het Comité I, wordt het begrip van inlichtingenofficier vervangen door "methodenofficier", zodat de titel van deze agent overeenstemt met de evolutie van zijn

compétences. Cet agent est en effet amené à remplir de plus en plus une fonction de gestion et de contrôle des différentes méthodes et non plus uniquement des BIM.

Ces officiers des méthodes sont responsables:

— du suivi de la méthode de recueil de données spécifique et/ou exceptionnelle (les méthodes appelées “BIM”),

— de tenir informé le dirigeant du service de l’exécution de la méthode.

L’officier de renseignement est visé expressément aux articles 18/3 (procédure pour mettre en œuvre une méthode spécifique) et 18/10 (procédure pour mettre en œuvre une méthode exceptionnelle).

En application de l’article 16/4, l’officier de renseignement peut également décider de l’accès aux données enregistrées depuis maximum un mois par les caméras de la police.

“L’officier de renseignement” est donc remplacé dans l’ensemble du texte par “l’officier des méthodes”.

“Faux nom”

L’article 2 insère une nouvelle définition portant sur le faux nom à l’article 3, 22°. Le faux nom est le fait de prendre un nom qui n’appartient pas à l’agent, sans que cela soit attesté par une carte d’identité, un passeport, une carte d’étranger ou un document de séjour ou par des documents officiels en découlant.

“Fausse qualité”

L’article 2 insère aussi une nouvelle définition portant sur la fausse qualité à l’article 3, 23°. Une fausse qualité est le fait de prendre une qualité qui n’appartient pas à l’agent et dont aucun effet juridique ne découle. Par exemple, lorsqu’un agent d’un service de renseignement se fait passer pour un chauffagiste ou un sociologue.

“Identité fictive”

Suite à l’avis du Comité R (point 54), l’article 2 introduit une nouvelle définition à l’article 3, 24° portant sur l’identité fictive.

bevoegdheden. Deze agent wordt er immers toe gebracht om steeds meer een beheer- en controlefunctie op de verschillende methodes uit te oefenen en niet slechts op de BIM’s.

Deze methodenofficiers zijn verantwoordelijk voor:

— de opvolging van specifieke en/of uitzonderlijke methoden voor het verzamelen van gegevens (de zogenaamde BIM-methoden);

— het op de hoogte houden van het diensthoofd van de uitvoering van de methode.

De inlichtingenofficier wordt uitdrukkelijk bedoeld in de artikelen 18/3 (procedure voor de aanwending van een specifieke methode) en 18/10 (procedure voor de aanwending van een uitzonderlijke methode).

Overeenkomstig artikel 16/4 kan de inlichtingenofficier ook beslissen over de toegang tot de gegevens die maximum één maand eerder door de politiecamera’s geregistreerd zijn.

“De inlichtingenofficier” wordt dus in de volledige tekst vervangen door “de methodenofficier”.

“Valse naam”

Aan de hand van artikel 2 wordt een nieuwe definitie toegevoegd aan artikel 3, 22° met betrekking tot de valse naam. De valse naam betreft het feit waarbij men een naam aanneemt die niet aan de agent toebehoort, zonder dat deze gestaafd wordt door een identiteitskaart, een paspoort, een vreemdelingenkaart of een verblijfsdocument of door officiële documenten die hieruit voortvloeien.

“Valse hoedanigheid”

Door artikel 2 wordt tevens een nieuwe definitie toegevoegd aan artikel 3, 23° met betrekking tot de valse hoedanigheid. Een valse hoedanigheid betreft het feit waarbij men een hoedanigheid aanneemt die niet aan de agent toebehoort en waaruit geen rechtsgevolgen voortvloeien, bijvoorbeeld wanneer een agent van een inlichtingendienst zich uitgeeft voor een verwarmingstechnicus of een socioloog.

“Fictieve identiteit”

Naar aanleiding van het advies van het Comité I (punt 54), wordt door artikel 2 een nieuwe definitie toegevoegd aan artikel 3, 24° met betrekking tot de fictieve identiteit.

En effet, la définition de l'identité fictive est essentielle pour distinguer son utilisation de celle du faux nom.

Les auteurs du présent projet ont cité de manière exhaustive les types de documents qui sont visés par ce concept: il s'agit des documents 'primaires' qui attestent légalement de l'identité de quelqu'un.

Dès lors, on entend par "identité fictive": "une fausse identité attestée par une carte d'identité, un passeport, une carte d'étranger ou un document de séjour".

Ces documents ont été choisis pour correspondre aux documents visés par l'article 6 § 1er de la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour.

Ainsi, l'infraction pénale d'usurpation d'identité (article 231 du Code pénal) ne s'appliquera pas là où l'utilisation d'une identité fictive est permise par la présente loi.

Bien entendu, dès qu'un des quatre documents précités a été 'confectionné', il convient de considérer que l'agent utilise une identité fictive, et ce, même s'il ne s'identifie pas directement, dans le cadre d'une opération, avec l'un de ces documents "primaires" (c'est-à-dire, une carte d'identité, un passeport, 'un titre de séjour ou une carte d'étranger) mais qu'il utilise un document qui en découle. Ainsi, par exemple, si l'agent s'identifie par un permis de conduire délivré sur base d'une carte d'identité contenant une fausse identité, il y a utilisation d'une identité fictive.

Ne sont par contre pas considérés comme une identité fictive:

1) l'utilisation de documents avec un faux nom qui ne s'appuient pas sur un des quatre documents précités (carte de légitimation, carte de visite…);

2) le travail des agents virtuels qui utilisent un faux nom ou un pseudonyme sans document officiel en attestant.

Ces exemples tombent eux sous le concept de faux nom (article 13/2).

De definitie van de fictieve identiteit is immers essentieel om een onderscheid te maken tussen dit begrip en dat van de valse naam.

De opstellers van dit ontwerp hebben alle soorten documenten waarop dit begrip van toepassing is op limitatieve wijze aangehaald: het gaat om 'primaire' documenten die de identiteit van een persoon wettelijk aantonen.

Hierdoor verstaat men onder "fictieve identiteit": "een valse identiteit, die wordt aangetoond door middel van een identiteitskaart, een paspoort, een vreemdelingenkaart of een verblijfsdocument".

Deze documenten werden gekozen omdat ze overeenstemmen met de documenten bedoeld in artikel 6 § 1 van de wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten.

Op die manier is er geen sprake van het strafbaar feit van identiteitsdiefstal (artikel 231 Strafwetboek) wanneer het gebruik van een fictieve identiteit toegestaan wordt door deze wet.

Natuurlijk dient ervan te worden uitgegaan dat de agent een fictieve identiteit gebruikt zodra één van vier voornoemde documenten 'vervaardigd' werd, en dit zelfs indien hij zich, in het kader van een operatie, niet rechtstreeks identificeert met één van deze 'primaire' documenten (met andere woorden een identiteitskaart, een paspoort, een verblijfsdocument of een vreemdelingenkaart), maar dat hij een document gebruikt dat hieruit voortvloeit. Zo is er bijvoorbeeld sprake van het gebruik van een fictieve identiteit wanneer de agent zich identificeert aan de hand van een rijbewijs dat werd afgeleverd op basis van een identiteitskaart met een valse identiteit.

Wordt daarentegen niet beschouwd als een fictieve identiteit:

1) het gebruik van documenten met een valse naam die niet gebaseerd zijn op een van de vier voornoemde documenten (legitimatiekaart, visitekaartje, …);

2) het werk van virtuele agenten die een valse naam of een pseudoniem gebruiken zonder een officieel document dat die naam of dat pseudoniem aantoont.

Deze voorbeelden vallen dan weer onder het begrip valse naam (artikel 13/2).

"Qualité fictive"

L'article 2 insère aussi une nouvelle définition portant sur la qualité fictive à l'article 3, 25°.

On entend par "qualité fictive": un statut, un titre ou une fonction n'appartenant pas à l'agent dont il découle des effets juridiques.

Exemples de qualité fictive: se déclarer propriétaire d'un bien, être diplomate, …etc. Dans ces situations, si un agent prend une de ces qualités, il en découlera des effets juridiques par rapport aux actes qu'il pose. S'il est propriétaire, il devrait pouvoir louer son bien, s'il est diplomate, il serait protégé par l'immunité diplomatique, …

Ainsi, pour répondre au point 54 de l'avis du Comité R, le simple fait d'omettre délibérément de révéler à un interlocuteur la qualité de membre d'un service de renseignement lors de la collecte de données n'est pas l'utilisation d'une qualité ou d'une identité fictive.

L'utilisation d'une identité et d'une qualité fictive dans le cadre d'une infiltration dans le monde virtuel étant un critère qui détermine le type de méthode à appliquer (ordinaire ou spécifique), leur définition était indispensable.

"Source humaine"

Pour répondre aux avis du Collège des procureurs généraux (point 3) et du Comité R (points 35, 36 et 72), une définition du concept de source humaine est introduite dans la loi à l'article 3, 26°. Par cette définition, le registre des sources humaines a donc un fondement légal.

Pour le reste, toute la procédure (y compris la personne compétente au sein du service de renseignement pour inscrire une personne comme source et les conditions pour être inscrite dans le registre des sources humaines) étant classifiée, elle se trouve dans la directive classifiée du 25 mars 2019 du Conseil National de Sécurité. Les autres clarifications demandées par le Comité R seront également introduites lors d'une prochaine adaptation de cette directive.

"S'infiltrer"

"Fictieve hoedanigheid"

Aan de hand van artikel 2 wordt tevens een nieuwe definitie toegevoegd aan artikel 3, 25° met betrekking tot de fictieve hoedanigheid.

Onder "fictieve hoedanigheid" moet worden verstaan: een statuut, een titel of een functie die niet toebehoort aan de agent en waaruit rechtsgevolgen voortvloeien.

Voorbeelden van een fictieve hoedanigheid: verklaren de eigenaar te zijn van een goed, zich uitgeven voor diplomaat, enz. Indien een agent zich in deze situaties één van deze hoedanigheden aanmeet, zullen hier ook rechtsgevolgen uit voortvloeien met betrekking tot de handelingen die hij stelt. Indien hij eigenaar is, zou hij zijn goed moeten kunnen verhuren; als hij diplomaat is, zou hij beschermd moeten worden door de diplomatieke onschendbaarheid, …

In antwoord op punt 54 van het advies van het Comité I wordt op deze manier het opzettelijk niet onthullen van de hoedanigheid van lid van een inlichtingendienst aan een gesprekspartner tijdens de verzameling van gegevens op zich niet beschouwd als het gebruik van een fictieve identiteit.

Aangezien het gebruik van een fictieve identiteit en hoedanigheid in het kader van een infiltratie in de virtuele wereld een criterium vormt voor de bepaling van het soort methode dat moet worden toegepast (gewoon of specifiek), is de definitie van deze begrippen onontbeerlijk.

"Menselijke bron"

In antwoord op de adviezen van het College van procureurs-generaal (punt 3) en van het Comité I (punten 35, 36 en 72), wordt een definitie van het begrip 'menselijke bron' ingevoegd in artikel 3, 26° van de wet. Door deze definitie heeft het register van de menselijke bronnen dus een wettelijke basis.

Verder is de volledige procedure (met inbegrip van de persoon die binnen de inlichtingendienst bevoegd is voor de inschrijving van een persoon als bron en de voorwaarden om ingeschreven te worden in het register van de menselijke bronnen) geclassificeerd en is dus terug te vinden in de geclassificeerde richtlijn van 25 maart 2019 van de Nationale Veiligheidsraad. De overige verduidelijkingen die gevraagd werden door het Comité I zullen eveneens ingevoegd worden tijdens de volgende aanpassing van deze richtlijn.

"Infiltreren"

Pour répondre à l'avis du Comité R, un nouveau point 27° est introduit à l'article 3 afin de définir l'infiltration. Les conditions pour être dans une infiltration, que ce soit dans le monde réel ou le monde virtuel, sont les suivantes:

1) c'est un agent spécifiquement désigné d'un service de renseignement et de sécurité qui s'infiltre,

2) l'infiltration a lieu en dehors des cas visés à l'article 18, cet article concernant le recours à des personnes dont des sources humaines pour collecter de l'information,

3) l'agent s'intègre délibérément dans un groupe ou dans la vie d'une personne:

La dimension délibérée exclut de l'infiltration les relations personnelles qu'un agent pourrait entretenir dans sa vie privée et qui pourraient lui donner accès à des informations utiles à l'exécution des missions des services de renseignement et de sécurité.

Cette condition implique que l'infiltration est une action planifiée des services de renseignement et de sécurité.

La dimension d'intégration signifie que l'agent infiltré entretient des relations interpersonnelles approfondies avec le milieu qu'il infiltre.

4) Le but sera de recueillir des informations ou des données, dans le cadre d'une enquête d'un service de renseignement et de sécurité et toujours dans l'intérêt de l'exercice des missions du service de renseignement et de sécurité concerné.

5) L'agent infiltré dissimulera sa qualité d'agent des services de renseignement et de sécurité et, pour les agents du Service Général du Renseignement et de la Sécurité, de membre du Ministère de la Défense.

Cette condition de dissimulation de la qualité d'agent consacre le caractère intrinsèquement clandestin de l'infiltration.

Plus spécifiquement, de par la nature et l'environnement de leurs missions, les agents du Service Général du Renseignement et de la Sécurité courent autant de risques en dévoilant qu'ils sont membres de la Défense en opération qu'en dévoilant leur qualité d'agent de renseignement. Ces dévoilements rendent l'infiltration dans le milieu visé impossible, d'où l'ajout de cette condition.

À titre d'exemple: un membre de la Défense déclaré comme tel ne peut pas espérer infiltrer un groupe

In antwoord op het advies van het Comité I wordt een nieuw punt 27° ingevoegd in artikel 3 om de infiltratie te definiëren. De toepassingsvoorwaarden voor een infiltratie, of het nu in de echte wereld is of in de virtuele wereld, zijn de volgende:

1) de infiltratie gebeurt door een agent van een inlichtingen- en veiligheidsdienst, die specifiek aangeduid is,

2) de infiltratie vindt plaats buiten de gevallen bedoeld bij artikel 18, dit artikel betreft het beroep doen op menselijke bronnen voor het verzamelen van informatie,

3) de agent integreert zich doelbewust in een groep of in het leven van een persoon:

Het element doelbewust sluit persoonlijke relaties die een agent zou kunnen hebben in zijn privéleven en die hem toegang zouden kunnen geven tot nuttige informatie voor de uitvoering van de opdrachten van de inlichtingen- en veiligheidsdiensten uit.

Deze voorwaarde impliceert dat de infiltratie een geplande actie is van de inlichtingen- en veiligheidsdiensten.

Het element van integratie betekent dat de infiltrerende agent diepgaande interpersoonlijke relaties onderhoudt met het milieu waarbinnen hij infiltreert.

4) het doel is om informatie of gegevens te verzamelen in het kader van een onderzoek door een inlichtingen- en veiligheidsdienst, en steeds in het belang van de uitoefening van de opdrachten van de betrokken inlichtingen- en veiligheidsdienst.

5) De infiltrerende agent verbergt zijn hoedanigheid van agent van de inlichtingen- en veiligheidsdiensten en, voor de agenten van de Algemene Dienste Inlichtingen en Veiligheid, van lid van het Ministerie van Defensie.

Deze voorwaarde van het verbergen van de hoedanigheid van de agent verwijst naar het intrinsieke clandestiene karakter van de infiltratie.

Meer in het bijzonder, omwille van de aard en de omgeving van hun opdrachten, lopen de agenten van de Algemene Dienst Inlichting en Veiligheid een even hoog risico indien ze onthullen dat ze lid zijn van Defensie in operatie, dan als ze hun hoedanigheid van inlichtingenagent onthullen. Deze onthullingen maken een infiltratie in het milieu onmogelijk, hetgeen de toevoeging van deze voorwaarde verklaart.

Als voorbeeld: een verklaard lid van Defensie zal niet kunnen hopen om te infiltreren in een

salafo-djihadiste lors d'une opération de lutte anti-terroriste à l'étranger. De surcroît, il sera une cible du simple fait d'être membre du détachement militaire belge.

De plus, l'agent devra:

a) soit participer ou faciliter les activités ou soutenir activement les convictions ou les activités de la personne ou du groupe qui fait l'objet de l'enquête.

b) soit entretenir des relations durables avec la personne ou le groupe.

Par cette condition de durabilité, les auteurs du projet de loi visent l'hypothèse suivante: un agent d'un service de renseignement belge qui développe délibérément une relation à long terme avec un agent de renseignement étranger, en pratiquant régulièrement des activités avec lui à titre privé, par exemple sportives. L'agent infiltré belge ne soutient pas les activités de l'agent étranger, ni ne partage ses convictions, mais pourra récolter de l'information pertinente pour ses missions grâce à la relation interpersonnelle qu'il aura développée et entretenue.

Le concept de "relation durable" sera précisé dans une directive sur l'infiltration dans le monde réel approuvée par le Conseil national de sécurité qui sera édictée afin de prévoir les modalités pratiques de l'infiltration, sur base des situations opérationnelles anticipées.

Ainsi, dans certaines situations particulières, une relation "intense" pourra être qualifiée de "durable". Il est concevable, par exemple, qu'une opération d'infiltration ne dure qu'une ou quelques semaines, mais implique un contact intensif.

Art. 3

Plusieurs modifications sont apportées à l'article 11.

Tout d'abord, deux corrections techniques sont apportées dans la version néerlandaise:

Les mots "*bedreigt of zou kunnen bedreigen*" sont placés après f) et le mot "*beheerst*" est remplacé par le mot "*beheert*".

La formulation de l'actuel point 2° du § 1er de l'article 11, lequel renvoie au respect des dispositions du droit des

salafistisch-djihadistische groep tijdens een operatie in de strijd tegen het terrorisme in het buitenland. Bovendien zal hij een doelwit worden wegens het loutere feit van lid te zijn van een Belgisch militair detachement.

Daarenboven dient de agent:

a) Ofwel deel te nemen aan de activiteiten of ze mogelijk maken, ofwel de overtuigingen of de activiteiten van de persoon of van de groep, die het voorwerp uitmaken van het onderzoek, actief ondersteunen.

b) Ofwel duurzame relaties te onderhouden met de persoon of de groep.

Via deze voorwaarde van duurzaamheid doelen de auteurs van dit wetsontwerp op de volgende hypothese: een agent van een Belgische inlichtingendienst die doelbewust een lange termijn relatie ontwikkelt met een agent van een buitenlandse inlichtingendienst door regelmatig privéactiviteiten met hem te doen, zoals bij voorbeeld sportactiviteiten. De infiltrerende Belgische agent ondersteunt noch de activiteiten van de buitenlandse agent, noch deelt hij de overtuigingen, maar zal pertinente informatie kunnen verzamelen voor zijn opdrachten dankzij de interpersoonlijke relatie die hij zal ontwikkeld en onderhouden hebben.

Het concept van "duurzame relatie" zal verder gedetailleerd worden in een richtlijn van de Nationale Veiligheidsraad omtrent infiltratie in de reële wereld, die zal opgesteld worden om de praktische modaliteiten van infiltratie te voorzien, op basis van verwachte operationele situaties.

Zo zal, in bepaalde bijzondere gevallen, een 'intensieve' relatie gekwalificeerd worden als 'duurzaam'. Het is bijvoorbeeld denkbaar dat een infiltratie-operatie maar een of enkele weken duurt, doch intensieve contacten behelst.

Art. 3

In artikel 11 worden verschillende wijzigingen aangebracht.

Vooreerst worden in de Nederlandstalige versie twee technische correcties aangebracht:

De woorden "bedreigt of zou kunnen bedreigen" worden na f) geplaatst en het woord "beheerst" wordt vervangen door het woord "beheert".

De huidige formulering van punt 2° van § 1 van artikel 11, waarin wordt verwezen naar de naleving van de

conflits armés, pouvait laisser supposer que la contre-attaque du SGRS ne pouvait intervenir qu'en cas de conflit armé lors duquel le droit des conflits armés est applicable. Tel n'est évidemment pas nécessairement le cas. Il peut y avoir des situations, en deçà du seuil d'application du droit des conflits armés, où une riposte légitime avec des moyens cyber peut avoir lieu, conformément aux règles du droit international.

Pour clarifier ce point, il est proposé de préciser qu'une contre-attaque avec des moyens cyber peut être menée, pour autant que cette dernière respecte les dispositions du droit international, conventionnel et coutumier, applicable, en ce compris le droit des conflits armés lorsque les critères d'applicabilité de ce dernier sont remplis. Ainsi, il est plus clair que la Défense peut utiliser sa capacité cyber offensive dans toutes les hypothèses où elle peut utiliser toutes ses autres capacités offensives.

A la demande du Centre pour la Cybersécurité Belgique (CCB), la Défense s'est engagée à mettre ses capacités cyber au service de la nation en cas de crise nationale de cybersécurité, si le cadre légal était adapté en ce sens. La modification proposée vise à fournir une base légale pour rendre possible cet appui à la nation.

Au point 11 de son avis, le Comité R déclare que c'est la première fois que le SGRS se voit confier une mission sans lien avec le domaine militaire. Pourtant, le SGRS a déjà pour mission de faire du renseignement relatif à toute activité qui pourrait menacer la sécurité des ressortissants belges à l'étranger et à toute activité des services de renseignement étrangers sur le territoire belge. Contrairement à ce que le Comité R déclare, ces deux missions n'ont aucun lien direct avec le domaine militaire.

En son point 11 toujours, le Comité R dit que pour que cette mission reste neutre budgétairement, il faudra fixer des priorités. Les auteurs du projet souhaitent attirer l'attention sur le fait que le SGRS ne devrait pas agir souvent sous couvert de cette mission et utilisera les moyens investis par la Défense pour le développement de la capacité cyber au profit des missions de la Défense.

Les auteurs du projet souhaitent également attirer l'attention du Comité R sur le fait que l'intervention du

bepalingen van het recht van de gewapende conflicten, kon doen veronderstellen dat de tegenaanval van de ADIV slechts mogelijk was bij een gewapend conflict waarbij het recht der gewapende conflicten van toepassing is. Dat is uiteraard niet noodzakelijk het geval, er kunnen zich situaties voordoen die onder de toepassingsdrempel van het recht der gewapende conflicten blijven, waarin een legitieme tegenaanval met cybermiddelen plaats kan vinden, overeenkomstig de regels van het internationaal recht.

Om dit punt te verduidelijken wordt voorgesteld om te preciseren dat een tegenaanval met cybermiddelen uitgevoerd mag worden, voor zover die in overeenstemming is met de bepalingen van het toepasselijke internationale recht, zowel het verdragsrecht als het gewoonterecht, met inbegrip van het recht der gewapende conflicten, indien aan de toepassingsvoorwaarden ervan voldaan is. Zo is het duidelijker dat Defensie haar offensieve cybercapaciteit kan gebruiken in dezelfde gevallen als die waarin ze haar andere offensieve capaciteiten kan gebruiken.

Op vraag van het Centrum voor Cybersecurity België (CCB) heeft Defensie zich ertoe verbonden haar cybercapaciteiten ten dienste van de natie te stellen in geval van een nationale cybersecuritycrisis, indien het wettelijke kader in die zin werd aangepast. De voorgestelde wijziging heeft tot doel een wettelijke basis te verschaffen om deze steun aan de natie mogelijk te maken.

In punt 11 van het advies verklaart het Comité I dat het de eerste keer is dat de ADIV zich belast ziet met een opdracht die geen link heeft met het militaire domein. Nochtans heeft de ADIV reeds de opdracht om inlichtingen te verzamelen betreffende elke activiteit die de veiligheid van de Belgische onderdanen in het buitenland zou kunnen bedreigen en elke activiteit van buitenlandse inlichtingendiensten op het Belgisch grondgebied. Deze twee opdrachten hebben, in tegenstelling tot hetgeen het Comité I beweert, geen direct verband met het militaire domein.

Nog steeds in zijn punt 11 stelt het Comité I dat het noodzakelijk is om prioriteiten te stellen opdat deze opdracht budgetneutraal zou blijven. De auteurs van het ontwerp wensen de aandacht te vestigen op het feit dat de ADIV -slechts zelden binnen het kader van deze opdracht zal moeten handelen en dat het de middelen welke geïnvesteerd werden door Defensie zal aanwenden voor de ontwikkeling van de cybercapaciteit ten voordele van de missies van Defensie.

De auteurs van het ontwerp wensen eveneens de aandacht van het Comité I te vestigen op het feit dat de

SGRS ne se situera pas nécessairement dans le cadre du droit de la guerre.

Le droit de la guerre n'est d'ailleurs d'application que lors des conflits armés (internationaux ou non-internationaux, chacun avec ses propres critères de qualification). Le fait que le droit de la guerre n'est pas nécessairement d'application lors des opérations cyber est également confirmé dans le renommé Manuel de Tallinn. Ce Manuel stipule qu'une opération cyber peut rendre le droit de la guerre applicable, mais uniquement pour autant que les critères classiques de qualification ont été remplis (voir entre autres Règle 82 et 83).

En son point 16, le Comité R se pose des questions sur la relation de cette nouvelle mission avec celles des autorités judiciaires.

Comme c'est également souvent le cas dans le cadre des autres missions du SGRS, il est évident qu'il y aura une coopération avec la Police fédérale en cas de crise cyber nationale, comme cela est d'ailleurs prévu dans le plan d'urgence cyber. Néanmoins, il n'y a pas d'ingérence dans les missions judiciaires car les objectifs sont différents. En tant que service de renseignement et de sécurité, la finalité du SGRS sera de mettre un terme le plus rapidement possible à la cyberattaque et de défendre les intérêts fondamentaux du pays. Pour ce faire, il est nécessaire d'identifier le plus rapidement possible l'origine de l'attaque.

Il est évident que les informations pertinentes récoltées par le SGRS seront transmises à la Police fédérale qui se chargera de rassembler les preuves et de poursuivre les auteurs des infractions. Les deux missions sont donc complémentaires.

Le plan d'urgence cyber sera d'office appliqué.

Afin de répondre à la demande du Comité R d'obtenir une clarification du cadre juridique qui doit être respecté lors de la mise en œuvre d'une telle cyber (contre) d'attaque, il suffit de faire référence aux règlements existantes: l'exécution d'une (contre) attaque par le SGRS (faisant partie des forces armées) ne sera possible que dans le cadre juridique existant de la mise en œuvre des forces armées (voir entre autres la loi du 20 mai 1994 relative aux périodes et aux positions des militaires du cadre de réserve, ainsi qu'à la mise en œuvre et à la mise en condition des Forces armées et l'arrêté royal du 6 juillet 1994 portant détermination des formes d'engagement opérationnel, d'assistance et d'appui militaire, et des activités préparatoires en vue de la mise en œuvre des forces armées).

tussenkomst van de ADIV zich niet noodzakelijk binnen het oorlogsrecht zal bevinden.

Het oorlogsrecht is immers enkel van toepassing tijdens gewapende conflicten (internationale of niet-internationale, elk met hun eigen specifieke kwalificatiecriteria). Dat het oorlogsrecht niet noodzakelijk van toepassing is tijdens cyberoperaties wordt eveneens bevestigd in de befaamde Tallinn Manual. In deze Manual wordt gesteld dat een cyber operatie binnen het toepassingsgebied van het oorlogsrecht kan vallen, doch enkel voor zover aan de klassieke kwalificatiecriteria werd voldaan (zie onder meer Regel 82 en 83).

Het Comité I stelt zich in punt 16 vragen over de verhouding tussen deze nieuwe missie en die van de gerechtelijke autoriteiten.

Zoals dat reeds vaak het geval is in het kader van de andere opdrachten van de ADIV, is het vanzelfsprekend dat er een samenwerking zal zijn met de Federale Politie in het geval van een nationale cybersecurity crisis, zoals dat trouwens voorzien is in het cybernoodplan. Er is echter geen inmenging in de gerechtelijke opdrachten aangezien de objectieven verschillend zijn. Als inlichtingen- en veiligheidsdienst zal de finaliteit van de ADIV erin bestaan om een cyberaanval zo snel mogelijk te stoppen en om de fundamentele belangen van het land te beschermen. Om dit te kunnen doen is het noodzakelijk om zo snel mogelijk de oorsprong van de aanval te identificeren.

Het spreekt voor zich dat de door de ADIV verzamelde relevante informatie overgemaakt zal worden aan de Federale Politie die belast zal zijn met het verzamelen van de bewijzen en het vervolgen van de daders van de misdrijven. Beide opdrachten zijn dus complementair.

Het cybernoodplan zal in elk geval toegepast worden.

Om de door het Comité I gestelde vraag tot verduidelijking van het wettelijke kader dat bij de uitoefening van een dergelijke cyber(tegen)aanval gerespecteerd moet worden te beantwoorden, kan verwezen worden naar de bestaande regelgeving: het uitvoeren van een (tegen) aanval door de ADIV (als deel van de krijgsmacht) zal slechts mogelijk zijn binnen het vastgelegde juridisch kader voor de aanwending van de krijgsmacht (zie hiervoor onder meer de wet van 20 mei 1994 betreffende de perioden en de standen van de militairen van het reservekader alsook betreffende de aanwending en de paraatstelling van de Krijgsmacht en het KB van 6 juli 1994 houdende bepaling van de vormen van operationele inzet , hulpverlening en militaire bijstand, en van de voorbereidingsactiviteiten met het oog op de aanwending van de krijgsmacht).

Ensuite, il convient de préciser que le point 2°/1 confie au SGRS la mission d'intervenir uniquement en cas de crise nationale de cybersécurité. Ceci n'exclut pas que le SGRS intervienne dans d'autres circonstances en qualité d'assistant technique, en appui des missions d'autres départements, en application de l'article 20.

Ce qu'il convient d'entendre par crise nationale de cybersécurité est défini au nouveau point 5° du § 2 de l'article 11. La définition découle de la notion de "crise" au sens de l'article 2 de l'arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise.

Cette notion de crise a d'ailleurs été reprise dans le plan d'urgence Cyber rédigé par le CCB (et est lui-même basée sur l'arrêté royal précité du 18 avril 1988).

Il faut entendre par "intérêts vitaux du pays ou les besoins essentiels de la population" auxquels renvoie cette notion:

— l'ordre public, c'est-à-dire la tranquillité, la salubrité et la sécurité publiques;

— le potentiel scientifique et économique du pays;

— la souveraineté nationale et les institutions établies par la Constitution et les lois;

— l'intégrité du territoire national.

Par ailleurs, l'intervention du SGRS se limite à tenter de neutraliser l'attaque, d'en identifier les auteurs et éventuellement de contre-attaquer dans le respect des règles de droit international.

Le Comité R recommande de remplacer "les intérêts vitaux du pays ou les besoins essentiels de la population" et de se concentrer sur les "infrastructures critiques" comme étant des entités à protéger (point 14 de son avis).

Selon le Comité, la définition choisie par les auteurs du projet serait trop large. Néanmoins, il convient de rappeler que la définition d'infrastructure critique dans la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques est la suivante: "installation, système ou partie de celui- ci, d'intérêt fédéral, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'interruption du fonctionnement ou la destruction aurait

Vervolgens dient er verduidelijkt te worden dat punt 2°/1 de opdracht om tussen te komen aan ADIV toevertrouwt, enkel in geval van een nationale cybersecurity crisis. Dit sluit niet uit dat de ADIV in andere omstandigheden technische bijstand verleent ter ondersteuning van opdrachten van andere departementen, overeenkomstig artikel 20.

Wat begrepen dient te worden onder nationale cybersecurity crisis is gedefinieerd in het nieuwe punt 5° van § 2 van artikel 11. Deze definitie is afgeleid van de notie "crisis" omschreven in artikel 2 van het koninklijk besluit van 18 april 1988 tot oprichting van het Coördinatie- en Crisiscentrum van de regering.

Deze definitie van crisis werd trouwens overgenomen in het door het CCB opgestelde cybernoodplan (en steunt zelf op het eerder vermelde koninklijk besluit van 18 april 1988).

Onder "vitale belangen van het land of essentiële behoeften van de bevolking" waarnaar dit begrip verwijst, moet het volgende worden begrepen:

— de openbare orde, dat wil zeggen de openbare rust, gezondheid en veiligheid;

— het wetenschappelijk en economisch potentieel van het land;

— de nationale soevereiniteit en de instellingen opgericht bij de Grondwet en de wetten;

— de integriteit van het nationaal grondgebied.

De tussenkomst van ADIV wordt trouwens beperkt tot het proberen te neutraliseren van de aanval, het identificeren van de daders en het eventueel uitvoeren van een tegenaanval in overeenstemming met het internationaal recht.

Het Comité I beveelt aan om "vitale belangen van het land of essentiële behoeften van de bevolking" te vervangen en in te zetten op de 'kritieke infrastructuren' als te beschermen entiteiten (punt 14 van het advies).

Het Comité meent dat de door de opstellers van het ontwerp gekozen definitie te ruim is. Niettemin, is het nuttig om te herhalen dat de definitie van kritieke infrastructuur in de wet van 1 juli 2011 betreffende de beveiliging en bescherming van de kritieke infrastructuren als volgt luidt: "installatie, systeem of een deel daarvan, van federaal belang, dat van essentieel belang is voor het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, en waarvan de verstoring van

une incidence significative du fait de la défaillance de ces fonctions".

Il n'est pas manifeste que la notion de "fonctions vitales de la société" soit moins large que la notion de "intérêts vitaux du pays". Si le Comité R fait référence aux listes des infrastructures critiques devant être établies par les autorités sectorielles, l'objectif n'est pas de limiter l'aide à la nation pouvant être apportée par le SGRS à des attaques sur des infrastructures exhaustivement énumérées.

Il est évident que si une cyberattaque répond à la définition de crise nationale cyber (notamment par la menace contre des intérêts vitaux), peu importe si le système faisant l'objet de l'attaque est dans la liste des infrastructures critiques, une réponse doit être donnée. Pour neutraliser l'attaque, l'État doit pouvoir bénéficier de l'expertise du SGRS.

Par ailleurs, les auteurs du projet ont fait le choix de maintenir une uniformité dans la définition de crise nationale pour éviter des applications différentes en fonction de l'application de la présente loi, de l'arrêté royal créant le Centre de crise et le plan d'urgence cyber.

Le Comité R recommande par ailleurs, au point 15 de son avis, de supprimer un des éléments de la définition de crise nationale de cyber sécurité, à savoir: "demande une action coordonnée de plusieurs départements et organismes". Les auteurs du projet sont d'opinion que cette condition est pertinente, d'un côté afin de garder la cohérence avec l'arrêté royal du 18 avril 1988 et de l'autre côté pour faire la différence avec les 'incidents' de cyber sécurité du plan d'urgence cyber qui ne remplissent pas les conditions cumulatives d'une 'crise nationale'.

Le but n'est en effet pas que le SGRS soit compétent pour tout incident mais seulement s'il s'agit d'une crise nationale nécessitant une telle coordination.

Le but de cet ajout est donc d'intervenir par certaines "actions cyber" en cas de crise nationale cyber. Cela ne porte en aucun cas atteinte aux compétences des deux services de renseignement de faire du renseignement "cyber".

Enfin, un point 6° est ajouté au § 1er pour viser toutes les autres missions qui sont confiées au SGRS par d'autres lois. Il s'agit de la même formulation qu'au point 4° de l'article 7 reprenant les missions de la Sûreté de l'État. Le SGRS se voit confier de plus en plus de missions dans d'autres lois: la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et

de werking of de vernietiging een aanzienlijke weerslag zou hebben doordat die functies ontregeld zouden raken".

Het is niet duidelijk of het begrip "vitale maatschappelijke functies" enger is dan het begrip "vitale belangen van het land". Wanneer het Comité I verwijst naar de lijsten van kritieke infrastructuren die door de sectorale autoriteiten moeten worden opgesteld, is het niet de bedoeling de bijstand aan de natie die de ADIV verleent, te beperken tot aanvallen op de infrastructuren die exhaustief opgesomd zijn.

Het is duidelijk dat indien een cyberaanval voldoet aan de definitie van een nationale cybercrisis (met inbegrip van een bedreiging van vitale belangen), een reactie noodzakelijk is, ongeacht of het aangevallen systeem opgenomen is in de lijst van kritieke infrastructuren. Om de aanval te neutraliseren, moet de staat gebruik kunnen maken van de deskundigheid van de ADIV.

Verder hebben de opstellers van het ontwerp gekozen voor uniformiteit in de definitie van nationale crisis, om te vermijden dat er verschillende toepassingen zouden ontstaan bij de toepassing van de huidige wet, het koninklijk besluit tot oprichting van het Crisiscentrum en het cybernoodplan.

Het Comité I stelt daarnaast, in punt 15 van het advies, voor om één van de elementen van de definitie van nationale cybersecurity crisis te schrappen; met name "de gecoördineerde inzet van verscheidene departementen en organismen vergt". De opstellers van dit ontwerp zijn van mening dat deze voorwaarde relevant is, enerzijds om de coherentie te bewaren met het koninklijk besluit van 18 april 1988 en anderzijds om het onderscheid te maken met de in het cybernoodplan bedoelde cybersecurity'incidenten' die niet voldoen aan de cumulatieve voorwaarden van een 'nationale crisis'.

Het doel is niet dat de ADIV bevoegd is voor elk incident, maar enkel voor een nationale crisis die een dergelijke coördinatie vereist.

De toevoeging strekt er derhalve toe om met bepaalde "cyberacties" tussen te komen in geval van een nationale cybersecurity crisis. Dit doet geenszins afbreuk aan de bevoegdheid van de twee inlichtingendiensten om "cyberinlichtingenwerk" te verrichten.

Tot slot is aan § 1 een punt 6° toegevoegd om te verwijzen naar alle andere taken die door andere wetten aan de ADIV zijn toevertrouwd. Dit is dezelfde formulering als punt 4° van artikel 7, dat betrekking heeft op de taken van de Veiligheid van de Staat. De ADIV krijgt steeds meer opdrachten in andere wetten: de wet van 11 december 1998 betreffende de classificatie en

avis de sécurité, la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, … L'intérêt de mentionner toutes ces missions complémentaires à l'article 11 est qu'il est alors possible de faire référence à l'ensemble des missions du SGRS par une seule disposition.

Une adaptation technique est apportée au § 3 en vue de viser également la nouvelle mission introduite au point 2°/1 du § 1er.

Au point 19 de son avis, le Comité R se demande ce que le SGRS pourrait exiger de la Sûreté de l'État en lien avec cette nouvelle mission. Le § 3 de l'article 11 précise que le SGRS peut requérir le concours de la Sûreté de l'État pour recueillir du renseignement. C'est donc également en ce sens qu'il faut lire l'ajout: le SGRS pourra par exemple demander à la Sûreté de l'État si une adresse IP utilisée dans l'attaque lui est connue. Il n'est donc question que de renseignement. Le § 3 ne donne évidemment pas le pouvoir au SGRS d'exiger que la Sûreté de l'État procède à une contre-attaque.

Art. 4

En application de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, la personne qui fait l'objet d'une enquête ou d'une vérification de sécurité doit au préalable donner son consentement. Ce consentement ne portant que pour la finalité de la délivrance d'une habilitation de sécurité ou d'un avis de sécurité, les services de renseignement et de sécurité ne peuvent pas utiliser les informations collectées pour d'autres finalités.

Néanmoins, lorsqu'un agent constate, dans le cadre d'une enquête ou d'une vérification de sécurité, des éléments indiquant une menace potentielle contre un intérêt fondamental de l'État, les auteurs du projet estiment que ces éléments doivent pouvoir être traités par le service compétent pour lutter contre ladite menace. Pour cette raison, il est inséré un nouvel alinéa à l'article 13 autorisant l'agent à transmettre l'information au dirigeant du service de renseignement et de sécurité auquel il appartient afin que l'information puisse être traitée pour lutter contre la menace, finalité différente de la finalité initiale (délivrance d'une habilitation ou d'un avis de sécurité).

Le dirigeant du service évalue les informations reçues. S'il constate qu'il y a bien une menace potentielle contre

veiligheidsmachtigingen, -attesten en -adviezen, de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren, de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid, enz. Het voordeel van al deze bijkomende opdrachten te vermelden in artikel 11 is dat het dan mogelijk is om naar alle opdrachten van de ADIV te verwijzen via deze één enkele bepaling.

Een technische aanpassing wordt aangebracht aan § 3 om ook de in punt 2°/1 van § 1 ingevoerde nieuwe opdracht weer te geven.

Het Comité I vraagt zich in punt 19 van het advies af wat de ADIV zou kunnen vereisen van de Veiligheid van de Staat in het kader van deze nieuwe missie. Artikel 11, paragraaf 3 bepaalt dat de ADIV de medewerking van de Veiligheid van de Staat kan vragen om inlichtingen te verzamelen. Het is dan ook in die zin dat de toevoeging gelezen moet worden: de ADIV kan bijvoorbeeld de Veiligheid van de Staat vragen of een bij een aanval gebruikt IP-adres bij hen bekend is. Het gaat enkel over inlichtingen. De § 3 geeft de ADIV uiteraard niet de bevoegdheid om te eisen dat de Veiligheid van de Staat tot een tegenaanval overgaat.

Art. 4

Op grond van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen moet de persoon die het voorwerp uitmaakt van een veiligheidsverificatie voorafgaand zijn instemming geven. Aangezien deze instemming enkel betrekking heeft op de afgifte van een veiligheidsmachtiging of een veiligheidsadvies, mogen de inlichtingen- en veiligheidsdiensten de verzamelde informatie niet voor andere doeleinden gebruiken.

Niettemin zijn de opstellers van het ontwerp van mening dat, wanneer een agent in het kader van een onderzoek of een veiligheidsverificatie elementen vaststelt, die wijzen op een potentiële dreiging tegen een fundamenteel belang van de Staat, deze elementen door de bevoegde dienst moeten kunnen worden behandeld om de dreiging in kwestie te bestrijden. Om deze reden wordt een nieuwe paragraaf ingevoegd in artikel 13 dat de agent toestaat de informatie over te maken aan het diensthoofd van de inlichtingen- en veiligheidsdienst waar hij toe behoort, zodat de informatie kan worden behandeld om de dreiging te bestrijden, hetgeen een andere finaliteit inhoudt dan de oorspronkelijke finaliteit (afgifte van een veiligheidsmachtiging of een veiligheidsadvies).

Het diensthoofd beoordeelt de ontvangen inlichtingen. Indien deze vaststelt dat er inderdaad een potentiële

un des intérêts fondamentaux visés aux articles 7 et 11 (les missions des deux services de renseignement et de sécurité) et/ou qu'il y a une menace potentielle (telle que définie à l'article 8) d'espionnage, de terrorisme, d'extrémisme, de prolifération, d'une organisation sectaire nuisible, d'une organisation criminelle ou d'ingérence, le dirigeant du service ayant reçu l'information la transmet au service compétent pour lutter contre la menace. Il peut s'agir par exemple de sections de son propre service, de l'autre service de renseignement et de sécurité ou de la police fédérale.

Art. 5

Le chapitre 3, section 2, est subdivisé en 4 sous-sections afin d'établir une distinction claire entre les différentes mesures de protection et d'appui:

— L'article 5 insère une sous-section 1 qui comprend les dispositions relatives aux causes d'excuse absolutoires pour la commission d'infractions par des agents et les sources humaines et la procédure à suivre;

— L'article 9 insère une sous-section 2 qui comprend les dispositions relatives à l'utilisation d'un faux nom et d'une fausse qualité et à l'utilisation d'une identité et d'une qualité fictives;

— L'article 11 insère une sous-section 3 qui comprend les dispositions relatives à la création et à l'utilisation des personnes morales;

— L'article 12 insère une sous-section 4 qui comprend les dispositions relatives à la coopération avec des tiers.

Art. 6 à 8

(Art. 13/1, 13/1/1, 13/1/2)

Actuellement, la loi prévoit déjà la possibilité pour les agents de commettre des infractions, comme mesure d'appui.

La nécessité s'impose toutefois d'étendre cette possibilité à d'autres situations afin de pouvoir mettre en œuvre une recommandation formulée par la Commission d'enquête parlementaire Attentats. En effet, afin de pouvoir intégrer de manière durable et anonyme des milieux dangereux, il est parfois nécessaire d'enfreindre le code pénal dans des situations dûment définies, par exemple pour prouver la crédibilité de l'agent ou de la source, ou pour maintenir la position d'information.

dreiging bestaat tegen een van de fundamentele belangen bedoeld in de artikelen 7 en 11 (de opdrachten van de twee inlichtingen- en veiligheidsdiensten) en/of dat er een potentiële dreiging is (zoals gedefinieerd in artikel 8) op het vlak van spionage, terrorisme, extremisme, proliferatie, een schadelijke sektarische organisatie, een criminele organisatie of inmenging, maakt het diensthoofd dat de inlichting heeft ontvangen deze over aan de dienst die bevoegd is voor de bestrijding van de dreiging. Het kan bijvoorbeeld gaan over secties van zijn eigen dienst, van de andere inlichtingen- en veiligheidsdienst of over de federale politie.

Art. 5

Hoofdstuk 3, afdeling 2 wordt onderverdeeld in 4 onderafdelingen zodat er een duidelijk onderscheid bestaat tussen de verschillende beschermings- en ondersteuningsmaatregelen:

— Artikel 5 voegt een onderafdeling 1 in die de bepalingen omvat over de strafuitsluitingsgronden voor het plegen van strafbare feiten door agenten en menselijke bronnen en de te volgen procedure;

— Artikel 9 voegt een onderafdeling 2 in die de bepalingen omvat over het gebruik van een valse naam en valse hoedanigheid en van de inzet van een fictieve identiteit en hoedanigheid;

— Artikel 11 voegt een onderafdeling 3 in die de bepalingen omvat over de oprichting en inzet van rechtspersonen;

— Artikel 12 voegt een onderafdeling 4 in die de bepalingen omvat over de medewerking van derden.

Art. 6 tot 8

(Art. 13/1, 13/1/1, 13/1/2)

De wet voorziet momenteel al in de mogelijkheid tot het plegen van inbreuken door de agenten, als steunmaatregel.

Het is echter noodzakelijk om deze mogelijkheid uit te breiden naar andere situaties, om zo een aanbeveling van de Parlementaire Onderzoekscommissie Aanslagen te kunnen uitvoeren. Immers, om zich op duurzame en anonieme wijze te kunnen begeven in gevaarlijke milieus, is het soms noodzakelijk om in welomschreven situaties de strafwet te overtreden, bijvoorbeeld om de geloofwaardigheid van de agent of bron te bewijzen of de informatiepositie te kunnen handhaven.

Les présentes modifications apportées à la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (ci-après “LRS”) introduisent:

— pour les agents des services de renseignement et de sécurité, un élargissement des possibilités de commettre des infractions dans le cadre de leurs missions;

— pour les sources humaines, la possibilité de commettre des infractions en vue d’améliorer ou de maintenir leur position d’informations ou de garantir leur propre sécurité lorsqu’ils travaillent en qualité de source humaine pour les services de renseignement et de sécurité.

Toutes ces infractions doivent toujours être directement proportionnelles à l’objectif visé par la mission de renseignement et ne peuvent en aucun cas porter atteinte à l’intégrité physique des personnes.

Les nouvelles dispositions insèrent des nouveaux paragraphes à l’article 13/1 de la LRS et des nouveaux articles 13/1/1 et 13/1/2.

Art. 6

Art. 13/1

Pour les agents

I. — **Cadre général**

1) ***La situation actuelle - le problème***

L’article 13/1 est déjà consacré à la commission d’infractions par les agents des services de renseignement et de sécurité dans le cadre de leurs missions.

Avant de commenter la nécessité des présentes modifications, il importe d’indiquer les possibilités qui existent actuellement en matière de commission d’infractions par les agents des services de renseignement et de sécurité prévues à l’article 13/1 de la LRS. Cet article est actuellement structuré comme suit:

— L’alinéa 1er de l’article 13/1 énonce en premier lieu le principe de l’interdiction de commettre des infractions pour les agents des services de renseignement et de sécurité.

— L’alinéa 2 énonce ensuite une cause d’excuse absolutoire concernant les contraventions, les infractions au code de la route ou le vol d’usage que l’agent peut commettre lorsqu’il exécute une méthode de recueil de

Deze wijzigingen, die aangebracht worden in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (hierna “WIV” genoemd), voorzien in de invoering:

— voor de agenten van de inlichtingen- en veiligheidsdiensten, van een uitbreiding van de mogelijkheden om in het kader van hun opdrachten strafbare feiten te plegen;

— voor de menselijke bronnen, van de mogelijkheid om strafbare feiten te plegen teneinde hun informatiepositie te verbeteren of te behouden of hun eigen veiligheid te garanderen, wanneer zij in de hoedanigheid van menselijke bron voor de inlichtingen- en veiligheidsdiensten werken.

Al die strafbare feiten moeten te allen tijde in gelijke verhouding staan tot het door de inlichtingenopdracht nagestreefde doel en mogen in geen geval afbreuk doen aan de fysieke integriteit van personen.

De nieuwe bepalingen voegen nieuwe paragrafen in in artikel 13/1 van de WIV alsook de nieuwe artikelen 13/1/1 en 13/1/2.

Art. 6

Art. 13/1

Voor de agenten

I. — **Algemeen kader**

1) ***Huidige situatie - het probleem***

Het artikel 13/1 is al gewijd aan het plegen van strafbare feiten door de agenten van de inlichtingen- en veiligheidsdiensten in het kader van hun opdrachten.

Alvorens de noodzaak van deze wijzigingen toe te lichten, dient gewezen te worden op de mogelijkheden die momenteel al bestaan op het vlak van het plegen van strafbare feiten door de agenten van de inlichtingen- en veiligheidsdiensten, bepaald in artikel 13/1 van de WIV. Dat artikel is momenteel als volgt gestructureerd:

— Het eerste lid van artikel 13/1 formuleert in de eerste plaats het principe van het verbod op het plegen van strafbare feiten voor de agenten van de inlichtingen- en veiligheidsdiensten.

— Het tweede lid formuleert vervolgens een strafuitsluitende verschoningsgrond voor overtredingen, inbreuken op de wegcode of een gebruiksdiefstal die de agent mag plegen wanneer hij een methode voor het

données, qu'elle soit ordinaire, spécifique ou exceptionnelle, et que les membres de l'équipe d'intervention peuvent également commettre dans le cadre de leur fonction.

— L'alinéa 3 de l'article 13/1 prévoit, lors de l'exécution des méthodes spécifiques et exceptionnelles, la possibilité pour les agents des services de renseignement et de sécurité de commettre des infractions absolument nécessaires afin d'assurer l'exécution optimale de la méthode spécifique ou exceptionnelle ou de garantir leur propre sécurité ou celle d'autres personnes.

— L'alinéa 4 prévoit la possibilité, dans des cas exceptionnels, de régulariser, a posteriori, une infraction commise par un agent, lorsque l'imprévisibilité et l'absolue nécessité pour garantir la sécurité des agents ou de tiers sont démontrées.

Toutes ces infractions doivent être directement proportionnelles à l'objectif visé par la mission de renseignement et ne peuvent en aucun cas porter atteinte à l'intégrité physique des personnes.

A l'exception des contraventions, des infractions au code de la route ou du vol d'usage prévus à l'alinéa 2, la commission d'infractions n'est donc prévue que dans le cadre des méthodes de recueil de données spécifiques et exceptionnelles (ci-après appelées les méthodes BIM). Dans cette hypothèse, la commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données (ci-après la Commission BIM) donne son accord dans le cadre de la procédure visant à mettre en œuvre une BIM.

Exception faite des contraventions, des infractions au code de la route ou du vol d'usage prévus à l'alinéa 2, il reste que rien n'est prévu en dehors de ces cas, notamment lorsque l'agent travaille dans le cadre d'une méthode de recueil de données ordinaire ou d'une méthode visée aux articles 44 à 44/2, ni s'il doit commettre une infraction absolument nécessaire pour l'achat de matériel. Le présent projet de loi vise à remédier à ce vide juridique et à permettre aux agents de pouvoir commettre des infractions absolument nécessaires afin d'assurer l'exécution optimale de leur mission ou de garantir leur propre sécurité ou celle d'autres personnes, lorsqu'ils récoltent des informations utiles pour le suivi des menaces fixées par la LRS.

Ce besoin de pouvoir commettre certaines infractions dans des situations spécifiques se fait sentir notamment dans le monde virtuel.

verzamelen van gegevens uitvoert, ongeacht of dit een gewone, specifieke of uitzonderlijke methode is, en die ook de leden van het interventieteam in het kader van hun functie mogen plegen.

— Het derde lid van artikel 13/1 voorziet, bij de uitvoering van de specifieke en uitzonderlijke methoden, in de mogelijkheid voor de agenten van de inlichtingen- en veiligheidsdiensten om strafbare feiten te plegen die strikt noodzakelijk zijn voor het welslagen van de uitvoering van de specifieke of uitzonderlijke methode of ter verzekering van hun eigen veiligheid of die van andere personen.

— Het vierde lid voorziet in de mogelijkheid om, in uitzonderlijke gevallen, een door een agent gepleegd strafbaar feit achteraf te regulariseren, als wordt aangetoond dat dit onvoorzienbaar en strikt noodzakelijk was om de veiligheid van agenten of derden te verzekeren.

Al die strafbare feiten moeten in gelijke verhouding staan tot het door de inlichtingenopdracht nagestreefde doel en mogen in geen geval afbreuk doen aan de fysieke integriteit van personen.

Behalve de overtredingen, inbreuken op de wegcode of een gebruiksdiefstal bepaald in het tweede lid, is enkel voorzien dat strafbare feiten gepleegd mogen worden in het kader van de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens (hierna BIM-methoden genoemd). In deze hypothese geeft de bestuurlijke commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens (hierna BIM-Commissie genoemd) haar toestemming in het kader van de procedure ter aanwending van een BIM.

Met uitzondering van de overtredingen, inbreuken op de wegcode of een gebruiksdiefstal bepaald in het tweede lid, is er buiten die gevallen nog niets bepaald, in het bijzonder wanneer de agent werkt in het kader van een gewone methode voor het verzamelen van gegevens of van een methode bedoeld in de artikelen 44 tot 44/2 en evenmin wanneer hij een strafbaar feit moet plegen dat absoluut noodzakelijk is voor de aankoop van materieel. Dit wetsontwerp beoogt dat juridisch vacuüm weg te werken en de agenten in staat te stellen strafbare feiten te plegen die strikt noodzakelijk zijn voor het welslagen van hun opdracht of ter verzekering van hun eigen of andermans veiligheid, wanneer zij informatie verzamelen die nuttig is voor de opvolging van de dreigingen die bij de WIV zijn vastgelegd.

Deze behoefte om in specifieke situaties bepaalde strafbare feiten te kunnen plegen is in het bijzonder merkbaar in de virtuele wereld.

Il est nécessaire, mais pas évident, pour les services de renseignement d'avoir accès aux forums et aux groupes de discussion sur l'internet où l'on partage aisément des menaces, des manuels et de la propagande, qui pourront ensuite être largement diffusés sur l'internet, de sorte que l'on ne sache plus qui est à l'origine de l'information.

Par le passé, les contenus djihadistes étaient massivement disponibles sur les chaînes publiques et il suffisait de créer un compte et de faire des recherches simples pour trouver du contenu à caractère terroriste: campagnes de recrutement, manuels pour fabriquer des explosifs, de préparation d'attentats, guides pour communiquer de manière discrète sur l'Internet ou pour faire la guerre médiatique, …

Suite à certains succès dans les rangs des services de renseignement et de sécurité, les membres des groupes terroristes ont commencé à limiter les accès aux fora en ligne. Les chaînes intéressantes sont devenues privées, il faut donc souvent recevoir une invitation pour y accéder et les administrateurs peuvent mettre un terme à un accès à tout moment. Ces invitations ne sont valables que pour une durée très limitée (de quelques minutes à quelques heures).

Cela signifie que les services de renseignement doivent être prêts à prouver leur crédibilité aux administrateurs. Il peut être nécessaire d'enfreindre la loi pour préserver la position d'information et la poursuite de l'enquête: apologie du terrorisme, diffamation, propos racistes, …

Si, en l'absence de crédibilité de leurs profils, ils ne sont que des "spectateurs", les services de renseignement peuvent rapidement être exclus des groupes, forums et canaux privés importants. La menace pour la sécurité nationale devient alors incontrôlable, et les services sont alors aveugles si un ou plusieurs individus manifestent leur volonté d'agir.

Afin de faciliter l'insertion dans de tels groupes de discussion, pouvoir partager de la propagande nazie ou salafo-djihadiste, partager des infographies (création d'images numériques assistée par ordinateur) de menaces (apologie du terrorisme), permettrait d'augmenter la crédibilité de la légende des profils des services de renseignement aux yeux de la mouvance salafo-djihadiste ou d'autres extrémistes. Ceci est absolument nécessaire afin de permettre la collecte, au sein de ces groupes, d'informations sur base de méthodes ordinaires.

Het is voor de inlichtingendiensten noodzakelijk, maar niet vanzelfsprekend, om toegang te krijgen tot fora en discussiegroepen op het internet waar men vlot bedreigingen, handleidingen en propaganda deelt, die vervolgens op grote schaal op het internet kunnen worden verspreid, waardoor niet meer duidelijk is wie aan de basis van die informatie ligt.

In het verleden was jihadistische content massaal beschikbaar via openbare kanalen en het volstond om een account aan te maken en eenvoudige opzoekingen te doen om content van terroristische aard te vinden: rekruteringscampagnes, handboeken voor de vervaardiging van springstoffen, handleidingen voor de voorbereiding van aanslagen en discrete internetcommunicatie of om mediaoorlogen te voeren, …

Naar aanleiding van bepaalde successen in de rangen van de inlichtingen- en veiligheidsdiensten zijn de leden van terroristische groeperingen begonnen met het beperken van de toegangen tot hun onlinefora. De interessante kanalen zijn privaat geworden, men moet dus vaak uitgenodigd worden om er toegang toe te krijgen en de administrators kunnen een toegang op ieder moment stopzetten. Die uitnodigingen blijven bovendien slechts voor een zeer beperkte duur (van enkele minuten tot enkele uren) geldig.

Dat maakt dat de inlichtingendiensten klaar moeten zijn om hun geloofwaardigheid te bewijzen ten opzichte van de administrators. Hierbij kan het noodzakelijk zijn om de wet te overtreden met het oog op het vrijwaren van de informatiepositie en de verderzetting van het onderzoek: verheerlijking van terrorisme, laster, racistische uitlatingen …

Indien ze, bij gebrek aan geloofwaardigheid van hun profielen, slechts"toeschouwers" zijn, kunnen de inlichtingendiensten snel worden uitgesloten van de belangrijke groepen, fora en privékanalen. De bedreiging voor de nationale veiligheid wordt dan oncontroleerbaar en de diensten zijn dan blind als een of meerdere personen zich bereid zouden tonen om tot actie over te gaan.

Om gemakkelijker in dergelijke chatgroepen opgenomen te worden, zou de mogelijkheid om nazistische of salafistisch-jihadistische propaganda te delen, om infographics (computerondersteunde digitale beeldcreatie) van dreigingen (verheerlijking van het terrorisme) te delen, de geloofwaardigheid van de dekmantel van de profielen waarachter de inlichtingendiensten schuilgaan verhogen in de ogen van de salafistisch-jihadistische beweging of van andere extremisten. Dit is absoluut noodzakelijk voor het verzamelen van informatie, binnen die groepen, op basis van gewone methoden.

Le monde virtuel déborde naturellement sur le monde réel. Il peut arriver qu'un agent, alors qu'il recueille des informations en ligne, se voit demander par un terroriste potentiel de rendre un service dans la vie réelle. Un exemple est l'agent virtuel à qui l'on demande d'aller chercher un colis et de le livrer quelque part, ou de transférer une petite somme d'argent. Accepter de fournir ce service peut apporter des informations précieuses sur les complices du terroriste potentiel. Actuellement, ce type de demande doit être rejeté car il est contraire à la loi. En conséquence, les services de renseignement perdent des informations précieuses.

Aussi, dans le monde réel, l'absolue nécessité de commettre une infraction apparaît également dans certains cas, en dehors des possibilités actuellement déjà prévues par l'actuel article 13/1.

Ainsi, pour collecter des informations indispensables dans le cadre d'une observation de lieux accessibles au public (méthode ordinaire - art. 16/1), les agents des services de renseignement peuvent être contraints de participer à une manifestation non autorisée organisée par un groupement extrémiste ou anarchiste. Afin de mieux se fondre dans la foule des manifestants, il pourrait être requis de porter une banderole avec des propos haineux (incitation à la haine).

Dans le cadre d'une observation (méthode ordinaire - art. 16/1), il peut aussi être indispensable qu'un agent porte un uniforme de police ou d'une société commerciale renommée pour passer inaperçu. Un autre exemple est une rencontre entre une source et un agent dans une brasserie (art. 18), au cours de laquelle tous deux sont contraints de quitter le bâtiment rapidement sans payer parce que des connaissances de la source arrivent soudainement. L'agent pourrait également se trouver dans une situation où, pour assurer la sécurité de tiers, il doive défoncer la barrière d'un parc fermé pour la nuit.

Par ailleurs, en ce qui concerne les méthodes visées aux articles 44, 44/1 et 44/2 permettant au SGRS de collecter à l'étranger via interception de communications, intrusion dans un système informatique ou prise d'image, il existe certaines circonstances qui peuvent justifier qu'un agent commette une infraction à l'étranger absolument nécessaire pour l'exécution de la méthode. Ainsi, il pourrait être absolument indispensable de pénétrer dans un lieu privé pour installer un micro, un dispositif technique dans un système informatique ou une caméra.

De virtuele wereld loopt uiteraard over in de echte wereld. Zo kan het gebeuren dat een agent, tijdens het online verzamelen van informatie, gevraagd wordt door een potentiële terrorist om een dienst in het echte leven te verlenen. Een voorbeeld hiervan is de virtuele agent aan wie gevraagd wordt een pakje op te halen en ergens af te leveren, of een kleine som geld over te schrijven. Het toestemmen om deze dienst te verlenen kan waardevolle informatie opleveren over de eventuele handlangers van de potentiële terrorist. Momenteel moet dit soort vragen afgewezen worden omdat het in strijd is met de wetgeving. Daardoor verliezen de inlichtingendiensten waardevolle informatie.

Ook in de echte wereld doet zich dus de strikte noodzakelijkheid een strafbaar feit te plegen zich in bepaalde gevallen voor, buiten de mogelijkheden die momenteel al in het huidige artikel 13/1 zijn bepaald.

Aldus kunnen de agenten van de inlichtingendiensten voor het verzamelen van onontbeerlijke informatie, in het kader van een observatie van voor het publiek toegankelijke plaatsen (art. 16/1), gedwongen zijn om deel te nemen aan een niet-toegestane manifestatie, georganiseerd door een extremistische of anarchistische groepering. Teneinde beter op te gaan in de menigte manifestanten, zou het noodzakelijk kunnen zijn om een spandoek met haatdragende uitlatingen te dragen (aanzetten tot haat).

In het kader van een observatie (gewone methode - art. 16/1) kan het ook onontbeerlijk zijn dat een agent een politie-uniform of een uniform van een bekend handelsvennootschap draagt om onopgemerkt te blijven. Een ander voorbeeld is een ontmoeting tussen een bron en een agent in een brasserie (art. 18), waarbij beiden gedwongen worden om snel het pand te verlaten zonder te betalen omdat plots bekenden van de bron opduiken. De agent zou zich ook in een situatie kunnen bevinden, waarin hij het hek moet intrappen van een park dat 's nachts gesloten is, en dit om de veiligheid van derden te garanderen.

Bovendien, wat de methoden bedoeld in artikelen 44, 44/1 en 44/2 betreft, die ADIV toelaten om via de interceptie van communicaties, het binnendringen in een informaticasysteem of het maken van beelden in het buitenland informatie te verzamelen, bestaan er bepaalde omstandigheden die kunnen rechtvaardigen dat een agent in het buitenland een strafbaar feit pleegt dat absoluut noodzakelijk is voor de uitvoering van de methode. Zo zou het absoluut onontbeerlijk kunnen zijn om een private plaats te betreden om er een micro, een technische voorziening in een informaticasysteem of een camera in aan te brengen.

Une exemption de peine, après accord bien entendu de la Commission, est nécessaire car l'article 10*bis* du titre préliminaire du Code de procédure pénale dispose que "*Toute personne soumise aux lois militaires qui aura commis une infraction quelconque sur le territoire d'un État étranger, pourra être poursuivie en Belgique.*" et l'article 14 continue: "*L'inculpé sera poursuivi et jugé d'après les dispositions des lois belges.*"

Il est évident que ce nouvel article 13/1 n'exemptera de peine les agents qu'en application de la loi belge, et que cela ne donnera pas de couverture en droit national du pays hôte (c'est également le cas pour d'autres articles de la LRS permettant certaines méthodes, notamment BIM, à l'étranger).

Il va de soi que toutes les actions entreprises par les agents des services de renseignement en dehors des frontières belges font l'objet d'une analyse de risque, visant à faire une balance d'intérêts entre les besoins en renseignement pour assurer la sécurité nationale et les risques encourus par les agents à l'étranger.

Le besoin de pouvoir commettre des infractions peut apparaître dans tout type d'enquête de renseignement, tant dans le cadre de la lutte contre le terrorisme, l'extrémisme ou le radicalisme, que dans le cadre de l'espionnage ou l'ingérence, mais aussi en lien avec l'appui en renseignement que le SGRS doit fournir aux opérations des Forces armées. Il est donc nécessaire de prévoir cette possibilité pour toutes les missions des deux services de renseignement (voir notamment les exemples fournis), à l'exception des enquêtes de sécurité, et également pour la sécurité des agents et des tiers.

Il convient également de rappeler que, conformément à l'alinéa 5 de l'article 13/1, devenu le paragraphe 8, l'infraction doit être directement proportionnelle à l'objectif visé par la mission de renseignement et ne peut en aucun cas porter atteinte à l'intégrité physique des personnes. Il appartiendra dès lors à la Commission d'évaluer la proportionnalité de l'infraction par rapport à l'objectif visé dans le cadre des différentes missions des services de renseignement et de sécurité.

2) ***La solution pour y remédier***

Les méthodes ordinaires et les méthodes visées aux articles 44 à 44/2 n'étant pas soumises à la Commission, une nouvelle procédure a été prévue pour obtenir l'autorisation de commettre une infraction. Elle est similaire à celle prévue dans le cadre des méthodes exceptionnelles.

Een vrijstelling van straf, welteverstaan na toestemming van de Commissie, is noodzakelijk omdat artikel 10*bis* van de voorafgaande titel van het Wetboek van Strafvordering bepaalt dat "*Ieder aan de militaire wetten onderworpen persoon die enig misdrijf pleegt op het grondgebied van een vreemde Staat, in België kan worden vervolgd.*" en artikel 14 vervolgt*: "De verdachte wordt vervolgd en gevonnist volgens de bepalingen van de Belgische wetten*".

Het is duidelijk dat het nieuwe artikel 13/1 de agenten van straf zal vrijstellen alleen in toepassing van de Belgische wetgeving, en dat dit geen dekking zal verlenen in de nationale wetgeving van het gastland (dit is ook het geval voor andere artikelen van de WIV die een aantal methoden toelaten, met name BIM's, in het buitenland).

Het spreekt voor zich dat alle acties die worden ondernomen door de agenten van de inlichtingendiensten buiten de Belgische staatsgrenzen, onderworpen zijn aan een risicoanalyse, gericht op het verkrijgen van een evenwicht tussen de inlichtingenbehoeften om de nationale veiligheid te verzekeren en de risico's die door de agenten in het buitenland opgelopen worden.

De noodzaak om misdrijven te kunnen plegen, kan zich voordoen bij elk soort inlichtingenonderzoek, of het nu in de strijd tegen terrorisme, extremisme of radicalisme is, of in de context van spionage of inmenging, maar ook in verband met de ondersteuning van inlichtingen die de ADIV moet verlenen aan de operaties van de strijdkrachten. Het is daarom noodzakelijk om in deze mogelijkheid te voorzien voor alle missies van de twee inlichtingendiensten (zie met name de gegeven voorbeelden), met uitzondering van de veiligheidsonderzoeken, en ook voor de veiligheid van de agenten en derde partijen.

Er moet aan worden herinnerd dat overeenkomstig artikel 13/1, lid 5, dat nu paragraaf 8 wordt, het strafbare feit rechtstreeks evenredig moet zijn met het doel van de inlichtingenopdracht en deze op geen enkele manier de fysieke integriteit van personen kan aantasten. Het is daarom aan de Commissie om de evenredigheid van het strafbaar feit te beoordelen in relatie tot het doel dat wordt nagestreefd in het kader van de verschillende opdrachten van de inlichtingen- en veiligheidsdiensten.

2) ***De oplossing om dit te verhelpen***

Gezien de gewone methoden en de in de artikelen 44 tot en met 44/2 bedoelde methoden niet aan de Commissie zijn onderworpen, moest dus een nieuwe procedure worden voorzien om de toelating te verkrijgen om een strafbaar feit te plegen. Deze procedure is vergelijkbaar met de procedure voor de uitzonderlijke methoden,.

Étant donné la lourde responsabilité d'une telle décision, et conformément aux règles constitutionnelles, un contrôle rigoureux sur la possibilité de commettre des infractions par les agents doit être opéré. C'est pourquoi le présent projet de loi prévoit plusieurs niveaux de contrôle pour encadrer une telle autorisation.

a) Procédure interne et décision du dirigeant du service

Dans le cadre d'une procédure interne avec plusieurs niveaux de validation, la demande d'autorisation de commettre une infraction sera élaborée par l'équipe ou l'agent responsable avant d'être soumise au dirigeant du service concerné. Cette demande sera toujours traitée par le dirigeant du service. Ce dernier sera aussi tenu informé lorsque l'infraction aura été commise.

b) Accord préalable de la Commission

Les membres de la Commission BIM, qui sont magistrats, ont été désignés pour assurer le rôle d'autoriser la commission d'infractions par les agents dans le cadre des missions des services de renseignement et de sécurité.

En effet, vu la grande responsabilité qu'implique l'autorisation de commettre des infractions et le fait que la Commission BIM est déjà compétente pour l'autoriser pour les agents dans le cadre de BIM, il a été décidé que ce soient les 3 magistrats qui la composent qui donnent leur accord préalable à la commission d'une infraction. Leur qualité de magistrats, leur connaissance approfondie du fonctionnement des services de renseignement et de sécurité et du droit pénal et le fait qu'ils sont organisés de manière à pouvoir répondre dans l'urgence si nécessaire, sont des compétences indispensables pour exercer un contrôle effectif sur l'autorisation de commettre des infractions.

L'appellation "commission" est utilisée pour la lisibilité du texte de loi. Elle fait référence à la commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles, visée à l'article 3, 6° de la LRS. Néanmoins, ce sont les magistrats visés à l'article 43/1 de la LRS, soit les membres de cette commission, qui sont visés car ils interviennent, dans le cadre du nouvel article 13/1, en dehors de toute méthode spécifique et exceptionnelle, alors que les compétences de la commission sont limitées aux méthodes spécifiques et exceptionnelles. La possibilité de commettre une infraction est une mesure de protection et d'appui, en vue de récolter de l'information, et non une méthode spécifique ou exceptionnelle. En leur qualité de magistrats, ils sont les mieux à même d'endosser le rôle d'autoriser une telle infraction.

Gezien de zware verantwoordelijkheid van een dergelijke beslissing en overeenkomstig de grondwettelijke regels moet er strikt toezicht uitgeoefend worden op de mogelijkheid van de agenten om strafbare feiten te plegen. Daarom voorziet dit wetsontwerp verschillende niveaus van toezicht tot regeling van een dergelijke toelating.

a) Interne procedure en beslissing van het diensthoofd

In het kader van een interne procedure met verschillende validatieniveaus, werkt het verantwoordelijke team of de agent de aanvraag voor een machtiging tot het plegen van een strafbaar feit uit alvorens het aan het betrokken diensthoofd wordt voorgelegd. Het diensthoofd behandelt altijd deze aanvraag en zal ook op de hoogte gehouden worden wanneer het strafbaar feit gepleegd is.

b) Voorafgaand akkoord van de Commissie

De leden van de BIM-Commissie, die magistraten zijn, werden aangewezen om de rol op te nemen om agenten toe te laten strafbare feiten te plegen in het kader van de opdrachten van de inlichtingen- en veiligheidsdiensten.

Gezien de grote verantwoordelijkheid die de toelating tot het plegen van strafbare feiten met zich meebrengt en het feit dat de BIM-Commissie reeds bevoegd is om dit toe te laten aan agenten in het kader van BIM's, werd beslist dat het de 3 magistraten die de commissie vormen zijn die hun voorafgaand akkoord voor het plegen van een strafbaar feit geven. Hun hoedanigheid van magistraat, hun grondige kennis van de werking van de inlichtingen- en veiligheidsdiensten en van het strafrecht en het feit dat ze zodanig georganiseerd zijn dat ze indien nodig met spoed kunnen reageren, zijn onontbeerlijke bekwaamheden om daadwerkelijk toezicht uit te oefenen op de toelating om strafbare feiten te plegen.

De benaming "commissie" wordt gebruikt om de leesbaarheid van de wettekst te vergroten. Het gaat om de bestuurlijke commissie belast met het toezicht op de specifieke en uitzonderlijke methoden, bedoeld in artikel 3, 6° van de WIV. Het zijn evenwel de magistraten bedoeld in artikel 43/1 van de WIV, d.w.z. de leden van die commissie, die bedoeld worden, aangezien zij, in het kader van het nieuwe artikel 13/1, optreden buiten de context van enige specifieke en uitzonderlijke methode, terwijl de bevoegdheden van de commissie beperkt zijn tot de specifieke en uitzonderlijke methoden. De mogelijkheid om een strafbaar feit te plegen is een beschermings- en ondersteuningsmaatregel, met het oog op het verzamelen van informatie, en geen specifieke of uitzonderlijke methode. In hun hoedanigheid van magistraten zijn ze het best geplaatst om de rol op zich te nemen om een dergelijk strafbaar feit toe te laten.

c) Contrôle du Comité permanent R

Afin que le Comité R puisse exercer un contrôle sur la commission d'infractions, il est informé de tous les accords donnés par la Commission. Le Comité R pourra également retirer l'accord donné par la Commission s'il estime que les conditions de l'article 13/1 ne sont pas remplies et si l'infraction n'a pas encore été commise.

II. — **La procédure d'autorisation détaillée**

Art. 13/1 § 1er

Tout d'abord, pour une meilleure clarté, l'article 13/1 est divisé en paragraphes plutôt qu'en alinéas.

Art. 13/1 § 2

L'alinéa 2 de l'article 13/1 devient le paragraphe 2.

Par ailleurs, pour tenir compte des avis du Conseil d'État (article 5 point 2) et du Collège des procureurs généraux (point 2.1), le paragraphe 2 est reformulé pour bien distinguer la commission d'infractions par un agent, chargé d'exécuter une méthode de recueil de données, d'un membre de l'équipe d'intervention, qui n'exécute pas de "méthode" mais assure l'exécution optimale d'une "mission". Cela rectifie ainsi une erreur de langage. Par ailleurs, le membre de l'équipe d'intervention agit toujours dans le cadre de ses missions légales prévues aux articles 22 à 35 de la LRS.

Art. 13/1 § 3

Le nouveau paragraphe 3 de l'article 13/1 prévoit que les agents, lors de l'exécution des missions visées aux articles 7, 1° et 3°/1 et 11§ 1er, 1° à 3° et 5° peuvent commettre des infractions mais uniquement avec l'accord préalable de la Commission. Ces infractions doivent être absolument nécessaires afin d'assurer l'exécution optimale de la mission ou pour garantir la sécurité des agents ou de tiers.

En reformulant ce paragraphe ainsi, les agents ont la possibilité de commettre des infractions dans les cas suivants:

— Dans le cadre des méthodes spécifiques et exceptionnelles, comme cela était déjà prévu dans l'ancien alinéa 3 de l'article 13/1;

c) Toezicht van het Vast Comité I

Opdat het Comité I toezicht kan uitoefenen op het plegen van strafbare feiten, wordt het geïnformeerd over alle toelatingen die gegeven worden door de Commissie. Het Comité I kan de door de Commissie gegeven toelating intrekken indien het de voorwaarden in artikel 13/1 niet vervuld acht en indien het strafbaar feit nog niet gepleegd werd.

II. — **De gedetailleerde toelatingsprocedure**

Art. 13/1 § 1

Eerst en vooral wordt artikel 13/1, ter verduidelijking, in paragrafen onderverdeeld in plaats van in leden.

Art. 13/1 § 2

Lid 2 van artikel 13/1 wordt paragraaf 2.

Verder wordt paragraaf 2, om rekening te houden met de adviezen van de Raad van State (artikel 5, punt 2) en van het College van procureurs-generaal (punt 2.1), geherformuleerd, zodat er een duidelijk onderscheid is tussen het plegen van strafbare feiten door een agent, belast met de uitvoering van een methode voor het verzamelen van gegevens, en een lid van het interventieteam, dat geen 'methode' uitvoert, maar de optimale uitvoering van een 'opdracht' verzekert. Op die manier wordt ook een taalfout gecorrigeerd. Het lid van het interventieteam handelt overigens steeds in het kader van zijn wettelijke opdrachten, zoals opgenomen in de artikelen 22 tot 35 van de WIV.

Art. 13/1 § 3

De nieuwe paragraaf 3 van artikel 13/1 voorziet dat de agenten, bij de uitvoering van de opdrachten bedoeld in artikelen 7, 1° en 3°/1 en 11, § 1, 1° tot 3° en 5°, strafbare feiten kunnen plegen, maar enkel met het voorafgaand akkoord van de Commissie. Deze strafbare feiten moeten absoluut noodzakelijk zijn voor het welslagen van de opdracht of ter verzekering van de veiligheid van de agenten of die van derden.

Door deze paragraaf als volgt te herformuleren hebben de agenten de mogelijkheid om strafbare feiten te plegen in de volgende gevallen:

— In het kader van de specifieke en uitzonderlijke methoden, zoals reeds bepaald in het derde lid van het oude artikel 13/1;

— Dans le cadre des méthodes ordinaires (comme par exemple, dans le cadre du travail des agents virtuels);

— Dans le cadre des méthodes visées aux articles 44 à 44/2 (méthodes mises en œuvre par le SGRS à l'étranger); et

— Dans le cadre de leurs missions, mais en dehors d'une méthode de recueil de données, comme par exemple, lors de l'achat de matériel illégal pour mener à bien une mission.

Pour répondre aux points 21 et 29 de l'avis du Comité R, la possibilité de commettre une infraction ne s'adresse pas uniquement aux agents qui collectent des informations mais à tout agent si la nécessité opérationnelle le justifie et que cela répond à toutes les conditions prévues dans le présent article. L'exemple précédent l'illustre d'ailleurs.

Les missions de la VSSE visées à l'article 7, 1° et 3°/1 excluent donc la possibilité de commettre des infractions dans le cadre des enquêtes de sécurité ou des autres missions confiées par ou en vertu d'une loi (4° de l'article 7).

Les missions du SGRS visées à l'article 11, § 1er, 1° à 3° et 5° excluent également la possibilité de commettre des infractions dans le cadre des enquêtes de sécurité.

Pour répondre au point 21 de l'avis du Comité R, il est rappelé que les deux services de renseignement et de sécurité font du renseignement afin d'assurer la sécurité des intérêts fondamentaux de l'État.

Toute mission de renseignement a comme finalité la sécurité nationale.

Par exemple, pour assurer la sécurité des intérêts militaires et protéger le secret, qui peuvent être menacés par tout type de menaces (espionnage, ingérence, terrorisme, extrémisme, organisation criminelle, …), le SGRS collecte de l'information, grâce aux différentes méthodes de recueil de données, et les analyse pour en faire du renseignement afin d'anticiper, dans la mesure du possible, toutes ces menaces.

Les exemples cités pour expliquer le besoin de commettre des infractions portent donc bien sur l'ensemble des missions du SGRS (sauf les enquêtes de sécurité exécutées en application de la loi du 11 décembre 1998).

— In het kader van de gewone methoden (bijvoorbeeld in het kader van het werk van de virtuele agenten);

— In het kader van de methoden bedoeld in de artikelen 44 tot 44/2 (door de ADIV aangewende methoden in het buitenland); en

— In het kader van hun opdracht, maar buiten de context van een methode voor het verzamelen van gegevens, zoals bijvoorbeeld bij de aanschaf van illegaal materieel om een opdracht tot een goed einde te brengen.

In antwoord op de punten 21 en 29 van het advies van het Comité I, is de mogelijkheid om een strafbaar pleit te plegen niet enkel bestemd voor agenten die inlichtingen verzamelen, maar voor elke agent, indien gerechtvaardigd door de operationele noodwendigheid en alle voorwaarden voorzien in dit artikel vervuld zijn. Het voorbeeld hierboven toont dit overigens aan.

De in artikel 7, 1° en 3°/1 bedoelde opdrachten van de VSSE sluiten derhalve de mogelijkheid uit om strafbare feiten te plegen in het kader van veiligheidsonderzoeken of andere opdrachten die bij of krachtens een wet zijn opgedragen (artikel 7, 4°).

De in artikel 11, § 1, 1° tot en met 3° en 5° bedoelde taken van de ADIV sluiten eveneens de mogelijkheid uit om in het kader van veiligheidsonderzoeken strafbare feiten te plegen.

In antwoord op punt 21 van het advies van het Comité I zij opgemerkt dat de twee inlichtingen- en veiligheidsdiensten inlichtingenwerk verrichten om de veiligheid van de fundamentele belangen van de Staat te verzekeren.

Elke inlichtingenopdracht heeft de nationale veiligheid tot doel.

Om, bijvoorbeeld, de veiligheid van de militaire belangen en de geheimhouding te vrijwaren, die door allerlei dreigingen bedreigd kunnen worden (spionage, inmenging, terrorisme, extremisme, criminele organisaties, …), verzamelt de ADIV informatie met de verschillende methoden voor het verzamelen van gegevens en analyseert deze informatie om ze om te zetten in inlichtingen, om zo in de mate van het mogelijke te anticiperen op al deze dreigingen.

De voorbeelden die werden aangehaald om de nood zaak van het plegen van strafbare feiten aan te tonen, hebben dus betrekking op het geheel van de opdrachten van de ADIV (met uitzondering van de veiligheidsonderzoeken die uitgevoerd worden op grond van de wet van 11 december 1998).

La commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles notifie son accord au dirigeant du service et au Comité permanent R.

Une limitation de la durée de l'accord a été prévue. L'accord ne peut porter que sur une période de maximum six mois. C'est un délai maximum qui doit être motivé sinon il pourra être refusé ou limité par la Commission. Ce délai s'explique non seulement par le temps nécessaire pour mettre en place les nécessités techniques ou de sécurité pour commettre l'infraction, mais également par le besoin de commettre des infractions continues ou une succession du même type d'infractions instantanées sur des durées relativement longues. A titre d'exemple, l'intégration dans un forum extrémiste prend du temps. Il s'agit de choisir le bon moment pour commettre ou répéter l'infraction, en respectant ainsi la proportionnalité. La possibilité de répéter l'infraction est utilisée avec précaution. Le rapport mensuel décrit, pour chaque infraction, les circonstances dans lesquelles celle-ci est commise. La répétition d'une infraction ne peut ainsi pas être considérée sans raison valable. L'agent est à tout moment conscient de la responsabilité engagée. Cela n'aurait pas d'utilité de contraindre un service de renseignement d'introduire des demandes similaires sur des périodes plus courtes, d'autant que la Commission sera tenue informée du déroulement de l'exécution de l'infraction toutes les deux semaines (voir le paragraphe 4).

Une demande de renouvellement de l'accord est possible en suivant la même procédure.

Les mentions prévues dans la demande signée par le dirigeant du service sont prescrites sous peine d'illégalité. Il est notamment exigé que le dirigeant précise la finalité pour laquelle l'infraction est demandée et motive la période demandée.

Les mots "les faits susceptibles d'être qualifiés infraction(s)" sont utilisés afin que la demande contienne les faits précis qui sont planifiés. Par contre, la qualification elle-même, qui n'entre pas dans les compétences d'un service de renseignement, est laissée à l'appréciation de la Commission.

Aussi, il n'est pas possible de mentionner l'identité d'un agent qui commettrait l'infraction. En effet, dans le monde virtuel, un profil peut être géré par plusieurs agents. Dans le monde réel, il n'est pas toujours possible de savoir à l'avance quel jour l'infraction pourra

De bestuurlijke commissie belast met het toezicht op de specifieke en uitzonderlijke methoden deelt haar akkoord mee aan het diensthoofd en aan het Vast Comité I.

Er wordt een beperking van de duur van het akkoord voorzien. Het akkoord kan slechts gelden voor een maximumperiode van zes maanden. Het gaat over een maximumtermijn, die gemotiveerd moet worden omdat hij anders door de Commissie geweigerd of beperkt kan worden. Deze termijn wordt niet alleen verklaard door de tijd die nodig is om de technische of veiligheidseisen die noodzakelijk zijn bij het plegen van het strafbaar feit vast te stellen, maar ook door de nood om voortdurende strafbare feiten te plegen of een opeenvolging van kortstondige strafbare feiten over relatief lange periodes. Als voorbeeld kan verwezen worden naar het binnendringen in een extremistisch forum, wat tijd kost. Het is ook een kwestie van het juiste moment te kiezen voor het begaan of herhalen van het strafbaar feit met inachtneming van het evenredigheidsbeginsel. De mogelijkheid om het strafbaar feit te herhalen wordt zorgvuldig gebruikt. Het maandelijks verslag beschrijft per strafbaar feit de omstandigheden waarin ze gemaakt is. Het herhalen van een overtreding kan enkel overwogen worden mits geldige reden. De agent is zich te allen tijden bewust van de aangegane verantwoordelijkheid. Het zou niet nuttig zijn om een inlichtingendienst te verplichten om meerdere soortgelijke verzoeken voor kortere perioden in te dienen, vooral omdat de Commissie om de twee weken op de hoogte zal worden gehouden van de voortgang van het strafbaar feit (zie paragraaf 4).

Een aanvraag voor verlenging van het akkoord is mogelijk door dezelfde procedure te volgen.

De vermeldingen die worden voorzien in het door het diensthoofd ondertekende verzoek, worden voorzien op straffe van onwettigheid. Er wordt met name vereist dat het diensthoofd aangeeft voor welk doel het strafbaar feit wordt gevraagd en dat hij de gevraagde periode motiveert.

De woorden "de feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd" worden gebruikt opdat het verzoek de specifieke feiten die gepland zijn, omvat. Anderzijds wordt de kwalificatie zelf, die niet onder de bevoegdheid van een inlichtingendienst valt, overgelaten aan het oordeel van de Commissie.

Het is evenwel niet mogelijk om de identiteit te vermelden van een agent die het strafbare feit zou plegen. Immers, in de onlinewereld kan een profiel door meerdere agenten worden beheerd. In de reële wereld is het niet altijd mogelijk om op voorhand te weten op welke dag

être effectivement commise et donc quel agent sera disponible ce jour-là.

Mais pour répondre au point 30 de l'avis du Comité R, une mention est ajoutée dans la demande. Elle vise à donner la liste des agents susceptibles de commettre les faits susceptibles d'être qualifiés infraction(s) visé au point 1°, en fonction du profil requis: formation, entrainement, expérience, apparence physique, maîtrise d'une langue, …

Pour répondre au point 32 de l'avis du Comité R, la mention visée au 6° est complétée pour utiliser la même formulation que dans les articles existants 18/3, § 2, 5° et 18/10, § 2, 5° LRS.

Pour répondre au point 31 de l'avis du Comité R, les mentions prévues à l'article 13/1 § 3 sont complétées par un 8°: le nom du ou des agent(s) chargé(s) du suivi du déroulement de l'infraction.

Art. 13/1 § 4

Ces infractions doivent toujours être directement proportionnelles à l'objectif visé par la mission et ne peuvent en aucun cas porter atteinte à l'intégrité physique des personnes.

Pour répondre à l'avis du Comité R en son point 22, il est certain que la loi sera respectée et que les agents ne commettront pas d'obstruction à la justice. Les agents seront par ailleurs encadrés par des instructions internes propres à chaque service de renseignement.

Article 13/1 § 5

Pour répondre à l'avis de la Commission BIM (p.2) concernant le § 5 de l'article 13/1, ce paragraphe est remanié pour plus de clarté.

Alinéa 1: de manière générale, l'agent qui assure le suivi du déroulement de l'infraction fait rapport par écrit au dirigeant du service le plus rapidement possible après la commission de l'infraction.

Par contre, les alinéas 2 et 3 distinguent deux situations différentes:

— l'alinéa 2 concerne l'hypothèse d'une infraction instantanée: le service de renseignement informera dans les plus brefs délais la Commission BIM.

— l'alinéa 3 vise l'hypothèse d'une infraction qui est autorisée pour une période supérieure à deux mois: dans ce cas, il est dérogé à l'alinéa 2 (et non à l'alinéa 1er comme prévu initialement) car le service de renseignement fait

het misdrijf daadwerkelijk zal worden gepleegd en dus welke agent beschikbaar zal zijn.

In antwoord op punt 30 van het advies van het Comité I, wordt echter een vermelding toegevoegd aan de aanvraag. Die strekt ertoe de lijst van agenten te geven die feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd, zoals bedoeld in punt 1°, kunnen plegen, op basis van het vereiste profiel: opleiding, training, ervaring, uiterlijk voorkomen, talenkennis, …

In antwoord op punt 32 van het advies van het Comité I wordt de vermelding bedoeld in 6° aangevuld, zodat dezelfde vermelding gebruikt wordt als in de bestaande artikelen 18/3, § 2, 5° en 18/10, § 2, 5° WIV.

In antwoord op punt 31 van het advies van het Comité I worden de vermeldingen voorzien in artikel 13/1 § 3 aangevuld met een 8°: de naam van de agent(en) belast met de opvolging van het verloop van het strafbaar feit.

Art. 13/1 § 4

Deze strafbare feiten moeten altijd in gelijke verhouding staan tot het door de opdracht nagestreefde doel en mogen in geen geval afbreuk doen aan de fysieke integriteit van personen.

In antwoord op punt 22 van het advies van het Comité I staat het vast dat de wet zal worden nageleefd en dat de agenten de rechtsgang niet zullen belemmeren. De agenten zullen overigens omkaderd worden door interne instructies eigen aan elk van de inlichtingendiensten.

Article 13/1 § 5

In antwoord op het advies van de BIM-Commissie (p. 2) met betrekking tot § 5 van artikel 13/1 werd deze paragraaf, met het oog op meer duidelijkheid, herschreven.

Lid 1: over het algemeen brengt de agent die het verloop van het strafbaar feit opvolgt zo snel mogelijk na het plegen van het strafbaar feit schriftelijk verslag uit aan het diensthoofd.

In de leden 2 en 3 wordt daarentegen een onderscheid gemaakt tussen twee verschillende situaties:

— lid 2 betreft de hypothese van een kortstondig strafbaar feit: de inlichtingendienst brengt de BIM-Commissie zo spoedig mogelijk op de hoogte.

— lid 3 betreft de hypothese van een strafbaar feit dat toegestaan werd voor een periode langer dan twee maanden: in dat geval wordt afgeweken van lid 2 (en niet van lid 1, zoals oorspronkelijk voorzien was), want

rapport à la Commission BIM toutes les deux semaines (au lieu de “dans les plus brefs délais”) sur le déroulement de l’exécution de l’infraction. Ainsi, les auteurs prévoient la même périodicité de rapportage (toutes les deux semaines) à la Commission BIM que pour les méthodes exceptionnelles.

En outre, le fait que la mesure puisse être autorisée sur une période supérieure à deux mois s’aligne sur la méthode exceptionnelle existante du recours à une personne morale (art. 18/13).

Cet alinéa 3 est également justifié par le fait que la possibilité de commettre une infraction par un agent peut être utilisée par les agents virtuels (voir le nouvel article 16/5). Ainsi, le nouveau paragraphe prévoit l’option d’indiquer une période durant laquelle l’infraction peut être commise. Ceci permet, par exemple, de donner une crédibilité virtuelle à un agent sans devoir à chaque fois demander l’autorisation pour “liker” une page internet prônant la violence. Comme indiqué ci-dessus, cette périodicité est inspirée du modèle du frontstore, visé à l’article 18/13 qui prévoit aussi une certaine période dans l’autorisation de créer une personne morale fictive.

Les rapports sont faits par écrit.

En outre, un alinéa 4 est ajouté pour qu’à la demande motivée de la Commission, le rapport puisse être transmis à plus courte échéance, tout en tenant compte des besoins opérationnels et en restant proportionnel et pour autant que l’agent soit en sécurité pour transmettre son rapport.

Article 13/1 § 6

Un nouveau paragraphe 6 est inséré à l’article 13/1, avec une procédure d’extrême urgence. Pour apporter une certaine uniformisation avec la procédure prévue en extrême urgence pour une méthode exceptionnelle (article 18/10 § 4), ce paragraphe 6 reprend les mêmes mécanismes.

Il est précisé que la confirmation écrite de la demande du dirigeant du service comprend les mentions visées au paragraphe 3, alinéa 4.

Pour suivre l’avis du Comité R (point 47), le paragraphe 6 est adapté afin qu’il soit conforme à la procédure d’extrême urgence en méthode exceptionnelle: “la Commission” a été remplacée par “le président ou le membre contacté” lors de la confirmation de son accord le plus rapidement possible.

de inlichtingendienst brengt om de twee weken verslag uit aan de BIM-Commissie (in plaats van “zo spoedig mogelijk”) over het verloop van de uitvoering van het strafbaar feit. Op die manier voorzien de auteurs dezelfde termijn (om de twee weken) voor de verslaglegging aan de BIM-Commissie voor de uitzonderlijke methoden.

Bovendien ligt het feit dat de maatregel toegestaan kan worden voor een periode langer dan twee maanden in de lijn van de bestaande uitzonderlijke methode waarbij men een beroep doet op een rechtspersoon (art 18/13).

Dit derde lid wordt verder gerechtvaardigd door het feit dat de mogelijkheid dat een agent een strafbaar feit pleegt, door de virtuele agenten kan worden gebruikt (zie het nieuwe artikel 16/5). Op die manier voorziet de nieuwe paragraaf de optie om een periode aan te duiden waarin het strafbaar feit kan worden gepleegd. Dit maakt het bijvoorbeeld mogelijk om een agent virtueel geloofwaardig te maken zonder dat hij elke keer de toelating moet vragen om een internetpagina die geweld predikt, te”liken”. Zoals hierboven aangegeven, is deze bepaling van een periode gebaseerd op het frontstoremodel, bedoeld in artikel 18/13, dat een bepaalde periode voorziet waarin het toegelaten is een fictieve rechtspersoon te creëren.

De verslagen worden schriftelijk uitgebracht.

Daarnaast wordt een vierde lid ingevoegd zodat, op gemotiveerd verzoek van de Commissie, het verslag op kortere termijn kan worden overgemaakt, rekening houdend met de operationele noden en de proportionaliteit en voor zover de agent in veiligheid is om zijn verslag uit te brengen.

Article 13/1 § 6

Een nieuwe paragraaf 6 met een hoogdringendheidsprocedure wordt in artikel 13/1 ingevoegd. Om deze procedure eenvormiger te maken met de procedure voorzien in geval van hoogdringendheid voor een uitzonderlijke methode (artikel 18/10 § 4) neemt deze paragraaf 6 dezelfde werkwijzen over.

Voorts wordt verduidelijkt dat de schriftelijke bevestiging van de vraag van het diensthoofd de vermeldingen bevat bedoeld in lid 4 van paragraaf 3.

In navolging van het advies van het Comité I (punt 47), wordt paragraaf 6 aangepast, zodat deze in overeenstemming is met de procedure voorzien in geval van hoogdringendheid voor een uitzonderlijke methode: “de Commissie” werd vervangen door “de voorzitter of het gecontacteerde lid” voor de zo spoedig mogelijke bevestiging van zijn akkoord.

Par ailleurs, l'accord donné par le magistrat contacté dans le cadre de la procédure d'extrême urgence ne peut pas être contredit par les autres magistrats. Contrairement à ce qui est indiqué au point 47 de l'avis du Comité R, la procédure d'extrême urgence est une exception au principe de la prise de décision de la Commission à la majorité des 2/3 car, vu l'urgence, on ne peut justement pas attendre l'issue de la décision collégiale. Par contre, une limite dans le temps de cet accord est introduite: l'accord ne vaut que pour cinq jours. Pendant ce temps, un accord peut être demandé à l'ensemble des trois magistrats dans le cadre de la procédure "normale" pour la période qui suit les cinq jours.

Pour répondre à l'avis de la Commission BIM sur ce point, celle-ci peut bien entendu toujours faire application de l'alinéa 2 du § 10: lorsqu'elle constate une illégalité, elle en informe le dirigeant du service concerné qui met fin à la mesure dès que possible.

Le Comité permanent R peut, quant à lui, retirer l'accord si l'infraction n'a pas encore été commise, en application du paragraphe 9.

Conformément à l'article 7, deuxième alinéa, du règlement intérieur de la Commission BIM du 3 mai 2016, les magistrats de la Commission sont disponibles et joignables en permanence. En cas d'application de la procédure d'urgence prévue au projet d'article 13/1 de la LRS (ainsi que dans le cadre de la procédure d'urgence existante dans le cas de méthodes exceptionnelles prévues à l'article 18/10, § 4 de la LRS), le président est le premier point de contact des services de renseignement et de sécurité. Un service de renseignement et de sécurité ne peut contacter un autre membre de la commission que lorsque le président n'est pas joignable. Le choix du membre à contacter dans ce cas, est préalablement déterminé par la Commission BIM elle-même et communiqué aux services. Par conséquent, les services de renseignement et de sécurité ne peuvent pas choisir quel autre membre ils peuvent contacter dans le cadre de la procédure d'urgence.

Une fois que le président ou l'autre magistrat contacté a pris une décision sur la question, la procédure proposée à l'article 13/1 de la LRS - tout comme la procédure existante à l'article 18/10, § 4 de la LRS - prévoit l'obligation pour le président ou l'autre magistrat contacté d'en informer immédiatement les autres membres de la Commission.

Art. 13/1 § 7

Enfin, la régularisation a posteriori des faits susceptibles d'être qualifiés infraction(s) absolument nécessaires

Voor het overige kan het akkoord van de magistraat die in het kader van de procedure van hoogdringendheid is gecontacteerd, niet door de andere magistraten worden tegengesproken. In tegenstelling tot hetgeen in punt 47 van het advies van het Comité I verklaard wordt, vormt de hoogdringendheidsprocedure een uitzondering op het besluitvormingsprincipe van de Commissie van een tweederdemeerderheid aangezien men, gezien de urgentie, juist niet kan wachten op een collegiale beslissing. Anderzijds wordt een tijdslimiet van dit akkoord ingevoerd: het akkoord is slechts vijf dagen geldig. Binnen die periode kan een akkoord worden gevraagd van alle drie magistraten volgens de 'normale' procedure voor de periode na deze vijf dagen.

In antwoord op het advies van de BIM-Commissie over dit punt, kan zij natuurlijk steeds toepassing geven aan het tweede lid van § 10: wanneer zij een onwettigheid vaststelt, brengt zij het betrokken diensthoofd hiervan op de hoogte, dat de maatregel zo snel mogelijk beëindigt.

Op grond van paragraaf 9 kan het Vast Comité I van zijn kant het akkoord intrekken indien het feit nog niet is gepleegd.

Overeenkomstig artikel 7, tweede lid van het Huishoudelijk Reglement d.d. 3 mei 2016 van de BIM-Commissie zijn de magistraten van de Commissie permanent bereikbaar en beschikbaar. Bij toepassing van de hoogdringendheidsprocedure in het ontworpen artikel 13/1 WIV (alsook in de bestaande hoogdringendheidsprocedure bij uitzonderlijke methoden voorzien in artikel 18/10, § 4 WIV) vormt de voorzitter het eerste aanspreekpunt voor de inlichtingen- en veiligheidsdiensten. Enkel wanneer de voorzitter niet kan gecontacteerd worden, kan een inlichtingen- en veiligheidsdienst een ander lid van de commissie contacteren. De keuze van het desgevallend te contacteren lid wordt vooraf bepaald door de BIM-Commissie zelf, en meegedeeld aan de diensten. De inlichtingen- en veiligheidsdiensten kunnen bijgevolg niet kiezen welk ander lid ze kunnen contacteren binnen de hoogdringendheidsprocedure.

Eenmaal de voorzitter of de andere gecontacteerde magistraat ter zake een beslissing heeft genomen voorziet de voorgestelde procedure in artikel 13/1 WIV – net zoals de bestaande procedure in artikel 18/10, § 4 WIV – de plicht in hoofde van de voorzitter of de andere gecontacteerde magistraat om de andere Commissieleden onmiddellijk van deze beslissing op de hoogte te brengen.

Art. 13/1 § 7

Ten slotte is het ook mogelijk om de feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd

et imprévisibles commis par un agent des services de renseignement et de sécurité est également possible, comme c'est déjà prévu pour la commission d'infractions dans le cadre d'une BIM (voir nouveau paragraphe 7 de l'article 13/1).

Pour répondre à l'avis de la Commission BIM (p.3), il est précisé que la notification du dirigeant du service à la Commission sera effectuée par écrit et dans les plus brefs délais et au plus tard dans les vingt-quatre heures qui suivent sa prise de connaissance de la commission des faits susceptibles d'être qualifiés infraction(s).

La possibilité d'obtenir la régularisation a posteriori des faits susceptibles d'être qualifiés infraction(s). n'est permise que si ces faits étaient absolument nécessaires pour garantir la sécurité des agents ou de tiers.

Il est précisé que la mesure d'appui de commission d'infraction(s) ne peut pas être mise en œuvre de manière autonome pour la collecte de données. Cela veut dire que ce n'est pas la commission de l'infraction qui a pour objet de collecter. Elle a pour but soit d'assurer la sécurité, soit d'appuyer une mission visée aux articles 7, 1° et 3°/1 et 11§ 1er, 1° à 3° et 5° de la LRS. Puisqu'il n'y a aucune donnée collectée directement au moyen de l'infraction, il n'y a pas la possibilité, pour le Comité permanent R, sauf en sa qualité d'autorité de protection des données (répond au point 27 de l'avis du Comité R), d'exiger la destruction des données lorsqu'une infraction n'aurait pas dû être commise.

Art. 13/1 § 8

Afin de tenir compte de la remarque du Comité R (point 34) et compte tenu de la protection des agents, les auteurs insèrent un nouveau paragraphe 8 qui permet au service de renseignement concerné de saisir le Comité R lorsque la Commission BIM a rendu une décision négative ou n'a rendu aucune décision dans le délai légal. Le Comité R décide alors s'il autorise, ou non, l'infraction.

En outre, un mécanisme similaire à ce qui est prévu à l'article 43/6, § 1er, alinéa 1 LRS (contrôle des BIM), est prévu à l'article 13/1, § 8, alinéa 2: en cas de décision négative, le Comité permanent R peut donner son accord s'il estime que les conditions de l'article 13/1 sont remplies.

die door een agent van de inlichtingen- en veiligheidsdiensten werden gepleegd, en absoluut noodzakelijk en onvoorzienbaar waren, achteraf te regulariseren, zoals dit reeds voorzien is voor de strafbare feiten die gepleegd worden in het kader van een BIM (zie nieuwe paragraaf 7 van artikel 13/1).

In antwoord op het advies van de BIM-Commissie (p.3), wordt verduidelijkt dat de kennisgeving van het diensthoofd aan de Commissie schriftelijk en zo spoedig mogelijk zal gebeuren, en dit ten laatste binnen de 24 uur vanaf zijn kennisname van het plegen van de feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd.

Deze mogelijkheid tot regularisatie na de feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd, wordt enkel toegestaan als deze feiten absoluut noodzakelijk waren om de veiligheid van de agenten of derden te garanderen.

Er wordt verduidelijkt dat de ondersteuningsmaatregel van het plegen van een strafbaar feit of strafbare feiten niet autonoom kan worden uitgevoerd voor het verzamelen van gegevens. Dit betekent dat geen strafbare feiten mogen gepleegd worden met als doel gegevens te verzamelen. Het heeft tot doel om de veiligheid te waarborgen of om een opdracht als bedoeld in artikelen 7, 1° en 3°/1 en 11, § 1, 1° tot 3° en 5° van de WIV te ondersteunen. Aangezien er geen rechtstreeks door het strafbare feit verzamelde gegevens zijn, heeft het Vast Comité I, behalve in zijn hoedanigheid van gegevensbeschermingsautoriteit (antwoord op punt 27 van het advies van het Comité I), niet de mogelijkheid om de vernietiging van de gegevens te eisen wanneer een strafbaar feit niet gepleegd had mogen worden.

Art. 13/1 § 8

Om rekening te houden met de opmerking van het Comité I (punt 34) en rekening houdend met de bescherming van de agenten, voegen de opstellers een nieuwe paragraaf 8 in, die de betrokken inlichtingendienst in staat stelt om het Comité I te vatten wanneer de BIM-Commissie een negatieve beslissing heeft uitgebracht of geen beslissing heeft uitgebracht binnen de wettelijke termijn. Het Comité I beslist dan of het strafbaar feit al dan niet toestaat.

Daarenboven wordt een mechanisme gelijkaardig aan hetgeen voorzien is in artikel 43/6, § 1, eerste lid van de WIV (controle op de BIM's) voorzien in artikel 13/1, § 8, tweede lid: in geval van een negatieve beslissing kan het Vast Comité I zijn akkoord geven indien het acht dat de voorwaarden van artikel 13/1 vervuld zijn.

Pour répondre à l'avis de la Commission BIM (p. 3-4), les auteurs du projet précisent que ce n'est pas une nouvelle compétence du Comité R puisqu'il peut déjà, en vertu de l'article 43/6, révoquer la décision de la Commission BIM, dans le cadre des BIM. En l'espèce, les auteurs du projet reproduisent cette compétence dans le cadre des articles 13/1 et 13/1/1 car à défaut, ces règles ne sont applicables que pour les BIM. Or, les auteurs souhaitent maintenir ce double contrôle pour une décision aussi sensible que d'autoriser une infraction.

Art. 13/1 § 9

Aussi, il est évident que le Comité permanent R peut exercer son pouvoir de contrôle général en application de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace et donc entendre toute personne qu'il estime nécessaire.

Art. 13/1 § 10

Enfin, le nouveau paragraphe 10 de l'article 13/1 prévoit l'obligation pour le dirigeant du service de renseignement et de sécurité concerné de révoquer la mesure dès que possible si l'absolue nécessité de commettre une infraction a cessé d'exister, si la mesure n'est plus utile pour atteindre l'objectif ou si une illégalité est établie. Le dirigeant du service informe la Commission et le Comité R de cette décision dans les meilleurs délais.

En outre, la Commission ou le Comité R, s'ils constatent une illégalité, en informe par écrit le dirigeant du service concerné qui met fin à la mesure prévue ou en cours dès que possible.

Cela répond dès lors à l'avis de la Commission BIM (p. 3), celle-ci peut en effet exiger du dirigeant du service concerné de mettre fin à la mesure en cours ou planifiée dès que possible si les conditions légales prévues à l'article 13/1 ne sont plus réunies.

En ce qui concerne la nécessité de la mesure pour assurer le succès de la mission, les auteurs du texte considèrent que le dirigeant du service concerné est mieux placé pour apprécier l'opportunité de mettre fin à la mesure si elle n'est plus utile pour atteindre l'objectif poursuivi.

In antwoord op het advies van de BIM-Commissie (p. 3-4), benadrukken de opstellers van het ontwerp dat het niet om een nieuwe bevoegdheid van het Comité I gaat, aangezien het krachtens artikel 43/6 de beslissing van de BIM-Commissie reeds kan intrekken in het kader van BIM's. In casu hernemen de opstellers van het ontwerp deze bevoegdheid in het kader van de artikelen 13/1 en 13/1/1, aangezien deze regels bij ontstentenis van deze vermelding enkel van toepassing zijn op BIM's. De opstellers wensen deze dubbele controle echter te behouden voor een beslissing die zo gevoelig is als het machtigen van een strafbaar feit.

Art. 13/1 § 9

Het is dan ook duidelijk dat het Vast Comité I zijn bevoegdheid tot algemene controle kan uitoefenen krachtens de wet van 18 juli 1991 op de controle van de politie- en inlichtingendiensten en het Coördinatieorgaan voor de dreigingsanalyse, en aldus alle personen die het noodzakelijk acht kan horen.

Art. 13/1 § 10

Tot slot voorziet de nieuwe paragraaf 10 van artikel 13/1 de verplichting voor het diensthoofd van de betrokken inlichtingen- en veiligheidsdienst om de maatregel zo snel mogelijk te beëindigen wanneer de absolute noodzaak voor het plegen van een strafbaar feit is weggevallen, wanneer de maatregel niet langer nuttig is voor het te bereiken doel of wanneer een onwettigheid wordt vastgesteld. Het diensthoofd brengt deze beslissing zo spoedig mogelijk ter kennis van de Commissie en het Comité I.

Bovendien stellen de Commissie en het Vast Comité I, wanneer zij een onwettigheid vaststellen, het betrokken diensthoofd hiervan schriftelijk in kennis, dat de geplande of lopende maatregel zo snel mogelijk beëindigt.

Dit beantwoordt bijgevolg aan het advies van de BIM-Commissie (p.3). Deze laatste kan immers van het diensthoofd eisen dat hij de geplande of lopende maatregel zo snel mogelijk beëindigt indien de wettelijke voorwaarden bedoeld in artikel 13/1 niet meer vervuld zijn.

Wat betreft de noodzakelijkheid van de maatregel voor het welslagen van de opdracht, beschouwen de opstellers van de tekst dat het betrokken diensthoofd het best geplaatst is om te beoordelen wanneer het gepast is om de maatregel te beëindigen indien deze niet langer nuttig is om het nagestreefde doel te bereiken.

Art. 13/1 § 11

Pour répondre aux points 24, 25 et 26 du Comité R et aux préoccupations de la Commission BIM concernant ses compétences de contrôle au cours de l'exécution de la mesure, un paragraphe 11 est inséré.

Les membres de la Commission pourront contrôler à tout moment la légalité des mesures.

Ils peuvent, à cet effet, avoir accès aux données relatives à la mesure, se saisir de toutes les pièces utiles et entendre les membres du service.

Les compétences de la Commission BIM dans le cadre d'une méthode exceptionnelle visée à l'article 18/10 § 6 ont donc été en grande partie reprises mais adaptées à la situation spécifique de la commission d'une infraction: si les auteurs ont voulu garder le même niveau de protection juridique que pour une méthode exceptionnelle, la procédure doit néanmoins être adaptée: il n'est en effet pas possible d'appliquer *mutatis mutandis* les mêmes compétences (comme par exemple, aller sur les lieux de l'infraction pour contrôler la légalité de la mesure).

Art. 13/1 § 11

In antwoord op de punten 24, 25 en 26 van het Comité I en op de bezorgdheden van de BIM-Commissie betreffende haar controlebevoegdheden in de loop van de uitvoering van de maatregel, wordt een paragraaf 11 ingevoegd.

De Commissieleden zullen op ieder moment de wettelijkheid van de maatregelen kunnen controleren.

Daartoe kunnen zij toegang krijgen tot de gegevens die betrekking hebben op de maatregel, zich alle nuttige stukken toe-eigenen en de leden van de dienst horen.

De bevoegdheden van de BIM-Commissie in het kader van een uitzonderlijke methode bedoeld in artikel 18/10 § 6 werden dus grotendeels hernomen, maar aangepast aan de specifieke situatie van het plegen van een strafbaar feit: hoewel de auteurs hetzelfde niveau van juridische bescherming hebben willen behouden als voor een uitzonderlijke methode, moet de procedure niettemin worden aangepast: het is immers niet mogelijk om dezelfde bevoegdheden (bijvoorbeeld naar de plaats van het strafbaar feit gaan om de wettelijkheid van de maatregel te controleren) *mutatis mutandis* toe te passen.

Art. 7

Art. 13/1/1

Pour les sources

I. — **Cadre général**

1) ***Situation actuelle – le problème***

Remarque préalable: Le 25 mars 2019, la directive relative au traitement des sources humaines par les services de renseignement et de sécurité a été approuvée, en exécution de l'article 18 de la LRS, par le Conseil National de Sécurité. Cette directive classifiée encadre le recours aux sources humaines. En outre, le recours aux sources humaines fait également l'objet d'instructions internes à chaque service de renseignement, instructions qui sont à la disposition du Comité permanent R.

Actuellement, les sources humaines qui travaillent avec les services de renseignement et de sécurité ne peuvent pas commettre d'infraction. Or, cette possibilité de commettre des infractions est devenue indispensable pour plusieurs raisons:

Art. 7

Art. 13/1/1

Voor de bronnen

I. — **Algemeen kader**

1) ***Huidige situatie – het probleem***

Voorafgaande opmerking: op 25 maart 2019 werd de richtlijn met betrekking tot de behandeling van menselijke bronnen door de inlichtingen- en veiligheidsdiensten, ter uitvoering van artikel 18 van de WIV, door de Nationale Veiligheidsraad goedgekeurd. Deze geclassificeerde richtlijn omvat het beroep op menselijke bronnen. Daarnaast is het beroep op menselijke bronnen ook het onderwerp van interne instructies bij elke inlichtingendienst, instructies die beschikbaar zijn voor het Vast Comité I.

Op dit ogenblik mogen de menselijke bronnen die met de inlichtingen- en veiligheidsdiensten samenwerken, geen strafbare feiten plegen. Deze mogelijkheid om strafbare feiten te plegen is echter onontbeerlijk geworden om verschillende redenen:

a) au regard de l'évolution de la législation en matière de terrorisme:

Le développement de la législation sur les infractions terroristes et l'élargissement de son champ d'application impliquent qu'un grand nombre de comportements constituent désormais une infraction. Ils ne peuvent donc pas être adoptés par les sources au risque qu'ils soient poursuivis pénalement.

Actuellement, comme tout fonctionnaire, les services de renseignement et de sécurité sont soumis à l'article 29 du Code d'instruction criminelle qui oblige un fonctionnaire à dénoncer tout fait délictueux dont il a connaissance à l'autorité judiciaire. Par conséquent, si les services de renseignement et de sécurité ont connaissance d'un tel fait, ils doivent le dénoncer aux autorités judiciaires.

À titre d'exemple, la mise à disposition d'un véhicule, le versement d'argent à une personne partie dans une zone djihadiste ou l'accès à un site de propagande payant n'est pas possible au regard de l'incrimination de la participation aux activités d'un groupe terroriste (article 140 du Code pénal), surtout en ce qui concerne "*la fourniture d'informations ou de moyens matériels au groupe terroriste, ou par toute forme de financement d'une activité du groupe terroriste, en ayant eu ou en ayant dû avoir connaissance que cette participation pourrait contribuer à commettre un crime ou un délit du groupe terroriste"*. Pourtant, la commission de tels actes pourrait permettre d'obtenir de nombreuses informations pertinentes et fiables.

b) afin d'assurer une position d'information et une crédibilité dans la collecte des informations.

En matière de terrorisme notamment, les sources humaines revêtent une importance capitale pour avoir une bonne position d'information. Or, pour asseoir sa crédibilité, la source doit parfois pouvoir commettre certaines infractions mineures mais qui pourront lui donner accès à des informations cruciales pour la détection de la menace. Cela est également important pour garantir la sécurité de la source.

La commission d'enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 à l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste, souligne "qu'il est important de renforcer la position d'information des services de renseignement, en accordant une attention particulière à un développement plus poussé des sources

a) gezien de evolutie van de wetgeving op het vlak van terrorisme:

De ontwikkeling van de wetgeving op terroristische misdrijven en de uitbreiding van het toepassingsgebied ervan houdt in dat een groot aantal gedragingen nu een strafbaar feit vormt. Deze gedragingen mogen dus niet door de bronnen gebruikt worden op gevaar af dat ze strafrechtelijk vervolgd worden.

Momenteel zijn de inlichtingen- en veiligheidsdiensten, zoals alle ambtenaren, immers onderworpen aan artikel 29 van het Wetboek van Strafvordering dat een ambtenaar verplicht om aan de gerechtelijke overheid bericht te geven van elk strafbaar feit waarvan hij kennis krijgt. Bijgevolg moeten de inlichtingen- en veiligheidsdiensten, indien ze kennis krijgen van een dergelijk feit, daarvan bericht geven aan de gerechtelijke overheden.

Bijvoorbeeld, het ter beschikking stellen van een voertuig, het storten van geld aan een persoon die naar een jihadistisch gebied is vertrokken of het toegang nemen tot een betalende site met propaganda, is niet mogelijk gezien het feit dat de deelname aan de activiteiten van een terroristische groep strafbaar gesteld is (artikel 140 van het Strafwetboek), vooral wat betreft "*het verstrekken van gegevens of materiële middelen aan een terroristische groep of door het in enigerlei vorm financieren van enige activiteit van een terroristische groep, terwijl hij wist of moest weten dat zijn deelname zou kunnen bijdragen tot het plegen van een misdaad of wanbedrijf door de terroristische groep*". Het stellen van dergelijke handelingen zou nochtans veel nuttige en betrouwbare informatie kunnen opleveren.

b) om de informatiepositie en de geloofwaardigheid bij de informatiegaring veilig te stellen.

Inzonderheid op het stuk van terrorisme zijn menselijke bronnen van kapitaal belang om een goede informatiepositie te hebben. Om haar geloofwaardigheid op te bouwen, moet de bron soms bepaalde lichte strafbare feiten kunnen begaan, die cruciale informatie voor het opsporen van de dreiging toegankelijk kunnen maken. Het is ook belangrijk om de veiligheid van de bron te waarborgen.

De parlementaire onderzoekscommissie belast met het onderzoek naar de omstandigheden die hebben geleid tot de terroristische aanslagen van 22 maart 2016 in de luchthaven Brussel-Nationaal en in het metrostation Maalbeek te Brussel, met inbegrip van de evolutie en de aanpak van de strijd tegen het radicalisme en de terroristische dreiging "benadrukt het belang van een versterking van de informatiepositie van de inlichtingendiensten, waarbij in het bijzonder aandacht moet worden

humaines (human intelligence) et à l'optimisation de l'accès aux canaux de communication des terroristes potentiels." (Rapport de la commission d'enquête parlementaire, p. 306).

Le présent projet de loi entend répondre pleinement à cette recommandation.

2) ***La solution pour y remédier***

Encore plus que pour les agents, une telle décision d'autoriser la commission d'infractions pour les sources humaines demande un contrôle strict et rigoureux. C'est pourquoi le présent projet de loi prévoit plusieurs niveaux de contrôle pour encadrer une telle autorisation:

a) Contrôle interne avant et après la décision

Le traitement des sources humaines, et donc également l'autorisation qui sera donnée de commettre une infraction, est assuré par des agents qui ont bénéficié d'une formation spéciale à cet effet, appelés officiers traitants.

Le traitement des sources humaines fait l'objet d'un contrôle interne sur l'intégrité physique, psychique et morale des sources. Est également prévu un contrôle exercé par la chaîne hiérarchique des officiers traitants.

Une procédure interne avec plusieurs niveaux de validation sera mise en place afin d'élaborer la demande d'autorisation de commettre une infraction par l'équipe ou l'agent responsable, avant d'être introduite auprès du dirigeant du service concerné.

b) Décision du dirigeant du service

La demande d'autorisation de commettre une infraction sera toujours décidée par le dirigeant du service. Ce dernier sera aussi tenu informé lorsque l'infraction aura été commise.

c) Accord préalable de la Commission

Le contrôle s'effectue par un accord préalable de la Commission.

Vu la grande responsabilité qu'implique l'autorisation de commettre des infractions et le fait que la Commission BIM est déjà compétente pour l'autoriser pour les agents dans le cadre de BIM, il a été décidé que ce soit cette

besteed aan een meer doorgedreven ontwikkeling van de human intelligence en aan de optimalisering van de toegang tot de communicatiekanalen van potentiële terroristen." (Verslag van de parlementaire onderzoekscommissie, blz. 306).

Dit wetsontwerp wil volledig tegemoetkomen aan deze aanbeveling.

2) ***De oplossing om dit te verhelpen***

Nog meer dan voor de agenten vereist dergelijke beslissing om menselijke bronnen machtiging te verlenen om strafbare feiten te begaan een strenge en nauwgezette controle. Daarom voorziet dit wetsontwerp in verschillende controleniveaus ter begeleiding van dergelijke machtiging:

a) Interne controle voor en na de beslissing

Voor de behandeling van de menselijke bronnen, en dus ook voor de machtiging die zal worden verleend om een strafbaar feit te begaan, hebben agenten die daartoe een bijzondere opleiding hebben genoten en behandelende officieren worden genoemd, de verantwoordelijkheid.

De behandeling van de menselijke bronnen wordt intern gecontroleerd op het stuk van de fysieke, psychische en morele integriteit van de bronnen. Er wordt ook voorzien in controle door de hiërarchische keten van de behandelende officieren.

Er zal een interne procedure met verschillende validatieniveaus worden ingevoerd waarbij het verantwoordelijke team of de verantwoordelijke agent de aanvraag om een strafbaar feit te mogen plegen, moet uitwerken alvorens het in te dienen bij het diensthoofd van de betrokken dienst.

b) Beslissing van het diensthoofd

Over het verzoek om machtiging om een strafbaar feit te begaan, wordt steeds beslist door het diensthoofd. Laatstgenoemde zal ook op de hoogte worden gehouden wanneer het strafbaar feit is begaan.

c) Voorafgaand akkoord van de Commissie

De controle wordt uitgevoerd met een voorafgaand akkoord van de Commissie.

Gelet op de grote verantwoordelijkheid die de machtiging tot het plegen van strafbare feiten inhoudt en het gegeven dat de BIM-Commissie reeds bevoegd is om in het kader van BIM's de agenten machtiging te verlenen,

même Commission qui autorisera, préalablement, la possibilité de commettre une infraction par une source. Leur qualité de magistrats, leur connaissance approfondie du fonctionnement des services de renseignement et de sécurité et du droit pénal et le fait qu'ils sont organisés de manière à pouvoir répondre dans l'urgence si nécessaire, sont des compétences indispensables pour exercer un contrôle effectif sur l'autorisation de commettre des infractions.

Il est à noter que dans la demande du dirigeant du service adressée à la Commission pour autoriser une infraction par la source sera incluse la synthèse de l'analyse de risques liée à la commission d'infraction envisagée. Les magistrats pourront, s'ils l'estiment nécessaire, consulter l'intégralité de l'analyse de risques liée à la commission de l'infraction envisagée.

d) Contrôle du Comité permanent R

Comme pour les agents dans le nouvel article 13/1, il est expressément prévu dans le nouvel article 13/1/1 que la décision d'autoriser à commettre une infraction soit notifié au Comité permanent R.

II. — **La procédure d'autorisation détaillée**

Art. 13/1/1 § 1er

En principe, il est interdit à la source humaine et aux officiers traitants concernés de commettre des infractions. Ce principe d'interdiction est repris au paragraphe 1er du nouvel article 13/1/1.

Art. 13/1/1 § 2

Néanmoins, vu la nécessité décrite ci-dessus, le présent projet de loi vise à introduire, au paragraphe 2 du nouvel article 13/1/1, une exemption de peine pour les sources humaines enregistrées dans le registre des sources humaines des services de renseignement et de sécurité (voir définition énoncée à l'article 3, 26°) qui commettent certaines infractions, en respectant des conditions strictes.

Les infractions ne peuvent être commises que dans le but d'assurer une position d'information par la source ou pour garantir sa propre sécurité ou celle d'autres personnes impliquées dans l'opération.

Il faut entendre par "assurer leur position d'information" le fait de conserver le contact, la relation que la source

werd beslist dat dezelfde Commissie voorafgaandelijk machtiging zullen verlenen om een bron de mogelijkheid te bieden om een strafbaar feit te begaan. Hun hoedanigheid van magistraat, hun grondige kennis van de inlichtingen- en veiligheidsdiensten en van het strafrecht en het gegeven dat zij dusdanig georganiseerd zijn dat zij bij hoogdringendheid een antwoord kunnen geven als het nodig is, zijn absoluut noodzakelijke competenties voor het uitoefenen van een effectieve controle op de machtiging om strafbare feiten te begaan.

Er moet worden opgemerkt dat in het verzoek van het diensthoofd dat aan de Commissie wordt gericht met het oog op het machtigen van de bron om een strafbaar feit te begaan, de synthese van de risicoanalyse in verband met het begaan van het beoogde strafbaar feit zal worden opgenomen. De magistraten kunnen, indien zij het nodig achten, de volledige risicoanalyse aangaande het voorziene strafbaar feit raadplegen.

d) Toezicht door het Vast Comité I

Net zoals voor de agenten in het nieuwe artikel 13/1, wordt in het nieuwe artikel 13/1/1 eveneens uitdrukkelijk bepaald dat de beslissing die een machtiging verleent om een misdrijf te plegen ter kennis wordt gebracht aan het Vast Comité I.

II. — **De machtigingsprocedure in detail**

Art. 13/1/1 § 1

In beginsel is het voor menselijke bronnen en de betrokken behandelende officier verboden om strafbare feiten te begaan. Dit verbod wordt opgenomen in paragraaf 1 van het nieuwe artikel 13/1/1.

Art. 13/1/1 § 2

Gelet op de hierboven beschreven noodzaak strekt dit wetsontwerp er niettemin toe in paragraaf 2 van het nieuwe artikel 13/1/1 een strafuitsluitingsgrond in te voegen voor de menselijke bronnen geregistreerd in het register van de menselijke bronnen van de inlichtingen- en veiligheidsdiensten (zie definitie in artikel 3, 26°), die bepaalde strafbare feiten plegen, met inachtneming van strikte voorwaarden.

De strafbare feiten mogen enkel begaan worden opdat de bron een informatiepositie zou kunnen veiligstellen of om zijn eigen veiligheid of die van andere personen die bij de operatie betrokken zijn, te verzekeren.

Onder het "veiligstellen van hun informatiepositie" moet worden verstaan het behoud van het contact, de

entretient avec la cible. Ainsi, ces raisons ne seront acceptées que si elles sont en lien avec leur fonction de source humaine travaillant pour un service de renseignement et de sécurité. Il est interdit d'autoriser des infractions qui porteraient atteinte à l'intégrité physique des personnes. Par ce biais, le projet de loi suit les remarques émises en 2007 par la Cour constitutionnelle (Cour constitutionnelle 19 juillet 2007, n°105/2007).

Pour répondre à l'avis du Comité R en son point 37, il est certain que la loi sera respectée et que les sources recevront comme instruction de ne pas faire obstruction à la justice. Elles seront par ailleurs encadrées par des directives internes propres à chaque service de renseignement et des instructions spécifiques à chaque opération fixéesdans le mémorandum visé à l'article 13/1/1 § 4.

Une cause d'excuse absolutoire est donc prévue expressément pour la source qui commet l'infraction avec l'accord préalable de la Commission.

L'accord ne peut porter que sur une période maximum de deux mois.

Les mentions prévues dans la demande signée par le dirigeant du service sont prescrites sous peine d'illégalité.

Les mots "les faits susceptibles d'être qualifiés infraction(s)" sont utilisés afin que la demande contienne les faits précis qui sont planifiés. Par contre, la qualification elle-même, qui n'entre pas dans les compétences d'un service de renseignement, est laissée à l'appréciation de la Commission qui est composée de magistrats.

En réponse au point 46 de l'avis du Comité R, l'échange d'informations se fera entre le Parquet et le service de renseignement concerné comme c'est déjà le cas lorsqu'une exemption de peine est applicable en vertu de la LRS (exemple: les infractions de roulage déjà prévues par la LRS). Il s'agit d'informations classifiées qui appartiennent au service. Pour ce faire, les services de renseignement ont une permanence 7 jours sur 7, 24h sur 24.

Les auteurs du projet sont également d'avis que des processus opérationnels seront développés avec les autorités judiciaires là où cela sera nécessaire, dans le cadre déjà existant de la circulaire confidentielle 02/2021 du Collège des procureurs généraux près les Cours d'appel qui régit la collaboration entre les autorités judiciaires et les services de renseignement.

relatie die de bron heeft met het doelwit. Die redenen zullen aldus enkel aanvaard worden indien zij verband houden met hun functie van menselijke bron die werkt voor een inlichtingen- en veiligheidsdienst. Het is verboden strafbare feiten te machtigen die de fysieke integriteit van personen zouden schenden. Zo volgt het wetsontwerp de opmerkingen die het Grondwettelijk Hof in 2007 maakte (Grondwettelijk Hof 19 juli 2007, nr. 105/2007).

In antwoord op punt 37 van het advies van het Comité I staat het vast dat de wet zal worden nageleefd en dat de bronnen de instructie zullen krijgen om de rechtsgang niet te belemmeren. Ze zullen overigens omkaderd worden door middel van interne richtlijnen eigen aan elk van de inlichtingendiensten en specifieke instructies voor elke operatie, die vastgelegd zijn in het memorandum bedoeld in artikel 13/1/1 § 4.

Er wordt dus uitdrukkelijk voorzien in een strafuitsluitende verschoningsgrond voor de bron die het strafbaar feit begaat met het voorafgaand akkoord van de Commissie.

Het akkoord mag slechts voor een maximumperiode van twee maanden gelden.

De vermeldingen die worden voorzien in het door het diensthoofd ondertekende verzoek, zijn voorgeschreven op straffe van onwettigheid.

De woorden "de feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd" worden gebruikt opdat het verzoek de specifieke feiten die gepland zijn, vermeldt. Anderzijds wordt de kwalificatie zelf, die niet onder de bevoegdheid van een inlichtingendienst valt, overgelaten aan het oordeel van de uit magistraten samengestelde Commissie.

In antwoord op punt 46 van het advies van het Comité I, gebeurt de uitwisseling van informatie tussen het Parket en de betrokken inlichtingendienst zoals dit reeds het geval is wanneer een strafuitsluiting van toepassing is krachtens de WIV (bijvoorbeeld: de verkeersovertredingen die al in de WIV voorzien zijn). Het gaat om geclassificeerde informatie die toebehoort aan de dienst. Hiertoe hebben de inlichtingendiensten een permanentie van 7 dagen op 7, 24 op 24 uur.

De opstellers van het ontwerp menen eveneens dat daar waar nodig operationele processen zullen worden ontwikkeld met de gerechtelijke overheden, binnen het reeds bestaande kader van de vertrouwelijke omzendbrief 02/2021 van het College van procureurs-generaal bij de hoven van beroep die de samenwerking regelt tussen de gerechtelijke overheden en de inlichtingendiensten.

La source humaine doit être enregistrée dans le registre des sources humaines des services de renseignement et de sécurité. Il faudra également respecter les instructions internes propres à chaque service de renseignement concerné, respecter les procédures prévues dans la directive du Conseil National de Sécurité conformément à l'article 18 de la LRS et toute la procédure stricte prévue par l'article 13/1/1 de la même loi. Celle-ci prévoit notamment comme obligation de faire une analyse de risques portant sur la fiabilité de la source et des risques que celle-ci encourt dans le cadre de la commission de(s) (l')infraction(s).

Pour répondre à l'article 6, point 2 de l'avis du Conseil d'État, l'analyse de risque(s) doit être réalisée préalablement à toute autorisation de commettre une infraction. Cette évaluation sera effectuée même en cas d'urgence.

Ainsi, il faut une décision motivée et écrite du dirigeant du service et l'accord préalable de la Commission pour que certaines infractions puissent être commises par les sources humaines.

Au point 25 de l'avis du Comité R, celui-ci compare la procédure à suivre pour l'infiltrant civil prévu à l'article 47 novies/1 du Code d'instruction criminelle avec le nouvel article 13/1/1.

Le Comité fait ici une comparaison entre les enquêtes de renseignement et les enquêtes pénales.

Les auteurs du projet sont d'avis que les finalités des deux types de procédures sont différentes. Le but de l'enquête de renseignement n'est pas de rassembler des preuves pour faire condamner quelqu'un. L'objectif est d'anticiper des menaces et de faire en sorte qu'elles ne se réalisent pas.

Les services de renseignement collectent de l'information, les services de police collectent des preuves. Les informations provenant des services de renseignement ne peuvent pas constituer les motifs exclusifs ni la mesure prépondérante conduisant à la condamnation d'une personne. Les éléments doivent être étayés de manière prédominante par d'autres éléments de preuve (voir notamment l'article 19/1 de la LRS du 30/11/1998 des services de renseignement qui le précisent expressément). C'est donc une restriction importante à la valeur probante des informations récoltées par les services de renseignement. Il existe donc un critère objectif raisonnablement justifié qui permet une différence de traitement entre les informations recueillies par les services de renseignement et les preuves récoltées par les services de police. Si le raisonnement avancé ici par le Comité R était retenu, cela reviendrait à considérer

De menselijke bron moet worden opgenomen in het register van de menselijke bronnen van de inlichtingen- en veiligheidsdiensten. Ook de interne instructies eigen aan elke betrokken inlichtingendienst, de procedures die in de richtlijn van de Nationale Veiligheidsraad overeenkomstig artikel 18 van de WIV zijn vastgelegd en de strikte procedure van artikel 13/1/1 van diezelfde wet moeten worden nageleefd. Het voorziet met name in een verplichting om een risicoanalyse uit te voeren met betrekking tot de betrouwbaarheid van de bron en de risico's waar zij zich aan blootstelt in het kader van het plegen van het strafbaar feit of de strafbare feiten.

In antwoord op artikel 6, punt 2 van het advies van de Raad van State moet de risicoanalyse worden uitgevoerd voorafgaand aan een machtiging voor het plegen van een strafbaar feit. Deze beoordeling zal zelfs in geval van hoogdringendheid worden uitgevoerd.

Zo is een schriftelijke met redenen omklede beslissing van het diensthoofd en het voorafgaande akkoord van de Commissie vereist vooraleer de menselijke bronnen bepaalde strafbare feiten kunnen begaan.

In punt 25 van het advies van het Comité I vergelijkt deze de te volgen procedure voor burgerinfiltratie voorzien in artikel 47 novies/1 van het Wetboek van Strafvordering met het nieuwe artikel 13/1/1.

Het Comité maakt hier een vergelijking tussen inlichtingenonderzoeken en strafonderzoeken.

De opstellers van dit ontwerp zijn van mening dat de doeleinden van beide procedures verschillend zijn. Het doel van een inlichtingenonderzoek is niet om bewijzen te verzamelen om iemand te laten veroordelen. Het doeleinde is te anticiperen op dreigingen en ervoor te zorgen dat die geen werkelijkheid worden.

De inlichtingendiensten verzamelen informatie, de politiediensten verzamelen bewijzen. De informatie die van de inlichtingendiensten komt, mag niet de enige grond noch de overheersende maatregel zijn voor de veroordeling van een persoon. De elementen moeten in overheersende mate steun vinden in andere bewijsmiddelen (zie inzonderheid artikel 19/1 van de wet houdende regeling van de inlichtingen- en veiligheidsdiensten van 30 november 1998, waarin dat uitdrukkelijk wordt bepaald). Het is dus een belangrijke beperking op de bewijskracht van de door de inlichtingendiensten verzamelde informatie. Er bestaat dus een redelijkerwijs gerechtvaardigd objectief criterium op basis waarvan een verschil in behandeling mogelijk is tussen de informatie die door de inlichtingendiensten is verzameld en de bewijzen die door de politie zijn verzameld. Als de redenering die het Comité I hier naar voren brengt, was

les services de police et de renseignement comme identiques alors que leur travail, leurs missions et leurs finalités sont différents.

Ceci a d'ailleurs été confirmé récemment par la Cour constitutionnelle dans un arrêt n° 64/2021 du 22 avril 2021 (question préjudicielle du Comité R). Il énonce notamment ce qui suit:

"B.10.1. Il ressort des travaux préparatoires de la loi du 4 février 2010 "que les finalités des services de renseignement et de sécurité diffèrent fondamentalement de celles des services de police, dans leur composante judiciaire" (*Doc. parl.*, Sénat, 2008-2009, n° 4-1053/1, p. 12).

Ainsi qu'il est exposé dans ces travaux préparatoires, le travail des services de renseignement et de sécurité est plutôt de nature analytique et vise à permettre de comprendre les structures et les réseaux présents en Belgique, alors que les autorités judiciaires et policières recherchent toujours des preuves liées à un fait punissable concret (déjà commis ou non). Dès lors, l'enquête pénale est toujours menée en vue de rechercher et de poursuivre des infractions qui ont été commises par des personnes déterminées, ou le seront, ou qui ont déjà été commises mais ne sont pas encore connues, alors que l'enquête de renseignement vise à recueillir des informations sur une série d'événements qui ne concernent pas forcément des faits punissables mais qui peuvent représenter un danger pour la sécurité de l'État, pour les intérêts militaires ou pour des intérêts fondamentaux du pays (ibid., p. 12).

La diversité de ces missions légales se reflète dans les natures clairement différentes des données recueillies dans les deux types d'enquêtes. La recherche de renseignements dans le cadre d'une information ou d'une instruction vise à recueillir des éléments de preuve concernant une infraction qui soient effectivement utilisables dans une procédure pénale devant le juge du fond. Les données que les services de renseignement et de sécurité recueillent ne visent pas à convaincre un juge du fond de la "culpabilité" pénale d'un prévenu mais à permettre à l'autorité publique de prendre les mesures qui s'imposent en vue de préserver les intérêts fondamentaux du pays. (…)".

Il en découle que la Cour a considéré que la différence de traitement entre ce qui était prévu par la loi du 30 novembre 1998 et ce qui était prévu dans le Code d'instruction criminelle repose sur une justification objective et raisonnable.

gevolgd, zou het erop neerkomen dat de politiediensten en de inlichtingendiensten als identiek worden beschouwd, terwijl hun werkzaamheden, opdrachten en doeleinden verschillend zijn.

Als antwoord op dat argument heeft het Grondwettelijk Hof ons standpunt bevestigd in een recent arrest nr. 64/2021 van 22 april 2021 (prejudiciële vraag van het Comité I). Daarin staat onder meer het volgende:

"B.10.1. Uit de parlementaire voorbereiding van de wet van 4 februari 2010 blijkt "dat de doelstellingen van de inlichtingen-en veiligheidsdiensten, op het vlak van het gerechtelijk werk, fundamenteel verschillen van die van de politiediensten" (*Parl. St.*, Senaat, 2008-2009, nr.4-1053/1, p.12).

Zoals in dezelfde parlementaire voorbereiding wordt uiteengezet, is het werk van de inlichtingen-en veiligheidsdiensten veeleer analytisch van aard en erop gericht inzicht te verwerven in de structuren en de netwerken die in België voorkomen, terwijl de gerechtelijke en politionele autoriteiten steeds bewijzen zoeken in verband met een (al dan niet reeds gepleegd) concreet strafbaar feit. Derhalve wordt het strafonderzoek steeds gevoerd met het oog op het opsporen en het vervolgen van misdrijven die door welbepaalde personen, hetzij zijn gepleegd, hetzij zullen worden gepleegd of reeds zijn gepleegd maar nog niet aan het licht zijn gekomen, terwijl een inlichtingenonderzoek strekt tot het verzamelen van informatie omtrent een reeks gebeurtenissen, die niet per definitie strafbare feiten betreffen, doch een gevaar kunnen betekenen voor de veiligheid van de Staat, voor de militaire belangen of voor fundamentele belangen van het land (ibid., p.12).

De onderscheidenheid van die wettelijke opdrachten komt tot uiting in de duidelijk verschillende aard van de in de beide types van onderzoek verzamelde gegevens. De zoektocht naar gegevens in het kader van een opsporings-of gerechtelijk onderzoek is erop gericht bewijselementen te verzamelen met betrekking tot een misdrijf, die daadwerkelijk bruikbaar zijn in een strafprocedure voor de rechter ten gronde. De gegevens die de inlichtingen-en veiligheidsdiensten verzamelen, strekken niet ertoe een rechter ten gronde te overtuigen van de strafrechtelijke "schuld" van een beklaagde, maar wel de overheid toe te laten de noodzakelijke maatregelen te nemen ter vrijwaring van de fundamentele belangen van het land (…)".

Daaruit blijkt dat het Hof van oordeel was dat het verschil in behandeling tussen wat door de wet van 30 november 1998 was bepaald en wat in het Wetboek van Strafvordering was bepaald, op een objectieve en redelijke rechtvaardiging berust.

Par ailleurs, de manière générale à travers plusieurs points de son avis (notamment aux points 25 alinéa 2, 39 alinéa 3 et 40), le Comité R compare l'équivalence ou la non-équivalence des procédures de contrôle. Pour ce faire, le Comité R semble ne pas tenir compte d'éléments importants.

La Commission BIM est composée de trois magistrats dont l'unique fonction est d'exercer un contrôle indépendant sur les méthodes BIM et les réquisitions de conservation généralisée et indifférenciée. Ces magistrats ne sont pas chargés de l'enquête et n'y sont d'aucune manière impliquée.

Par ailleurs, il convient de rappeler que le Comité permanent R, qui est également un organe de contrôle indépendant, exerce un contrôle effectif sur toutes les méthodes de recueil de données par les services de renseignement, ce qui n'est pas le cas du Comité permanent P qui n'exerce pas de contrôle sur les méthodes de collecte utilisées lors d'enquêtes pénales. En outre, l'Organe de contrôle de l'information policière ne contrôle pas le Procureur du Roi et le juge d'instruction. Le dirigeant d'un service de renseignement est, quant à lui, contrôlé par le Comité R, tant dans sa fonction d'organe de contrôle des services de renseignement, que dans sa fonction d'Autorité de protection des données.

Afin de répondre aux avis de la Commission BIM (pp.1-2) et du Collège des procureurs généraux (point 2.2), les auteurs du projet souhaitent préciser qu'en ce qui concerne la possibilité pour une source de commettre une infraction, il a été décidé d'en faire une mesure d'appui plutôt qu'une méthode exceptionnelle car l'exemption de peine qui est prévue pour la source ne vise pas à collecter de l'information. La mesure d'appui vient soutenir la méthode ordinaire visée à l'article 18. La finalité de la mesure vise à protéger la source ou à renforcer sa crédibilité. Ceci étant, vu la lourde responsabilité qu'implique l'autorisation de commettre une infraction, les auteurs du projet ont souhaité encadrer cette possibilité avec les garanties de contrôle les plus poussées, comparables à celle d'une méthode de recueil de données exceptionnelle. Ainsi, comme pour une méthode exceptionnelle, l'autorisation préalable de la Commission BIM est obligatoire pour qu'une source humaine puisse commettre une infraction.

Comme pour le nouveau paragraphe 3 de l'article 13/1, l'appellation "commission" est utilisée pour la lisibilité du texte de loi. Elle fait référence à la commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles, visée à l'article 3, 6° de la LRS.

Voorts vergelijkt het Comité I in het algemeen in verschillende punten van zijn advies (met name de punten 25, lid 2, 39, lid 3, en 40) de gelijkwaardigheid of niet-gelijkwaardigheid van de controleprocedures. Daarbij lijkt Comité I geen rekening te houden met belangrijke elementen.

De BIM-commissie is samengesteld uit drie magistraten met als enige functie onafhankelijk toezicht te houden op de BIM-methoden en de vorderingen tot de algemene en ongedifferentieerde bewaring. Die magistraten zijn niet belast met het onderzoek en zijn er op geen enkele manier bij betrokken.

Voorts moet erop worden gewezen dat het Vast Comité I, dat ook een onafhankelijk controleorgaan is, daadwerkelijk toezicht uitoefent op alle methoden voor het verzamelen van gegevens door de inlichtingendiensten, en dat het Vast Comité P geen toezicht uitoefent op de tijdens strafrechtelijke onderzoeken gebruikte verzamelmethoden. Bovendien controleert het Controleorgaan op de politionele informatie de procureur des Konings en de onderzoeksrechter niet. Het hoofd van een inlichtingendienst wordt gecontroleerd door Comité I, zowel in diens functie van orgaan voor de controle op de inlichtingendiensten als in diens functie van gegevensbeschermingsautoriteit.

In antwoord op het advies (pp. 1-2) van de BIM-Commissie en van het College van procureurs-generaal (punt 2.2) wensen de opstellers van het ontwerp te verduidelijken dat wat de mogelijkheid voor een bron om een strafbaar feit te plegen betreft, er beslist werd om hiervan een ondersteuningsmaatregel te maken in plaats van een uitzonderlijke methode, aangezien de strafuitsluiting die voorzien is voor de bron niet gericht is op de verzameling van informatie. De ondersteuningsmaatregel ondersteunt de gewone methode bedoeld in artikel 18. Het doeleinde van de maatregel is gericht op de bescherming van de bron of de versterking van zijn betrouwbaarheid. Dat gezegd zijnde, gezien de zware verantwoordelijkheid verbonden aan de machtiging voor het plegen van een strafbaar feit, wensten de opstellers van het ontwerp deze mogelijkheid te omkaderen met de meest doorgedreven garanties op het stuk van controle, vergelijkbaar aan die van een uitzonderlijke methode voor het verzamelen van gegevens. Net als voor een uitzonderlijke methode is de voorafgaande toestemming van de BIM- commissie vereist opdat een menselijke bron een strafbaar feit kan plegen.

Net als in de nieuwe paragraaf 3 van artikel 13/1 wordt de benaming "commissie" gebruikt om de leesbaarheid van de wettekst te vergroten. Het gaat om de bestuurlijke commissie belast met het toezicht op de specifieke en uitzonderlijke methoden, bedoeld in artikel 3, 6° van de

Néanmoins, ce sont les magistrats visés à l'article 43/1 de la LRS, soit les membres de cette commission, qui sont visés car ils interviennent dans le cadre du nouvel article 13/1/1, en dehors de toute méthode spécifique et exceptionnelle, alors que les compétences de la commission sont limitées aux méthodes spécifiques et exceptionnelles. La possibilité de commettre une infraction est une mesure de protection et d'appui, en vue de récolter de l'information, et non une méthode spécifique ou exceptionnelle. En leur qualité de magistrats, ils sont les mieux à même d'endosser le rôle d'autoriser une telle infraction.

Pour répondre aux points 23, 25 et 26, § 3 de l'avis du Comité R, les auteurs du projet ont souhaité se rapprocher le plus possible des possibilités de contrôle accordées à la Commission BIM en matière de BIM, tout en l'adaptant aux spécificités de cette mesure d'appui qu'est la commission d'une infraction.

Pour répondre aux points 23 et 26 de l'avis du Comité R, il est rappelé que si des données sont collectées illégalement, ce sont les règles applicables à la méthode utilisée qui s'appliqueront: s'il s'agit d'une méthode spécifique ou exceptionnelle, la Commission BIM pourra effectivement suspendre la méthode et interdire l'exploitation des données et le Comité R pourra ordonner leur destruction.

Si l'infraction est commise dans le cadre d'une méthode de recueil de données et que l'infraction est irrégulière, la régularité de la méthode elle-même doit bien entendu être réévaluée.

Pour répondre au 1er tiret des remarques de la Commission BIM concernant le nouvel article 13/1/1 (p.4), la demande du dirigeant du service mentionne également la synthèse de l'analyse de risque(s) portant sur la fiabilité de la source et les risques qu'elle encourt dans le cadre de la commission de(s) (l')infraction(s). Celle-ci inclut l'évaluation de sa personnalité, de ses antécédents judiciaires, sa motivation, …

Par ailleurs, le contenu de l'analyse de risques et son résumé seront détaillés dans la mise à jour de la directive du Conseil National de sécurité du 25 mars 2019.

Art. 13/1/1 § 3

Ces infractions doivent nécessairement être proportionnelles à l'objectif et doivent entrer dans le cadre de la mission du service concerné.

WIV. Het zijn evenwel de magistraten bedoeld in artikel 43/1 van de WIV, d.w.z. de leden van die commissie, die bedoeld worden, aangezien zij, in het kader van het nieuwe artikel 13/1/1, optreden buiten de context van enige specifieke en uitzonderlijke methode, terwijl de bevoegdheden van de commissie beperkt zijn tot de specifieke en uitzonderlijke methoden. De mogelijkheid om een strafbaar feit te begaan is een beschermings- en ondersteuningsmaatregel met het oog op het verzamelen van informatie, en geen specifieke of uitzonderlijke methode. In hun hoedanigheid van magistraten zijn ze het best geplaatst om de rol op zich te nemen om een dergelijk strafbaar feit te machtigen.

In antwoord op de punten 23, 25 en 26 § 3 van het advies van het Comité I wensten de opstellers van het ontwerp zo dicht mogelijk te naderen bij de controlemogelijkheden toegekend aan de BIM-Commissie voor wat BIM's betreft, maar ze aan te passen aan de specifieke kenmerken van deze ondersteuningsmaatregel bestaande uit het plegen van een strafbaar feit.

In antwoord op de punten 23 en 26 van het advies van het Comité I zij het opgemerkt dat indien de gegevens onwettig verzameld worden, de regels gelden die van toepassing zijn op de gebruikte methode: indien het gaat om een specifieke of uitzonderlijke methode zal de BIM-Commissie de methode effectief kunnen opschorten en de exploitatie van de gegevens verbieden en het Comité I zou de vernietiging ervan kunnen bevelen.

Indien het strafbaar feit gepleegd wordt in het kader van een methode voor het verzamelen van gegevens en het strafbaar feit onwettig is, moet de regelmatigheid van de methode zelf uiteraard opnieuw beoordeeld worden.

In antwoord op de tekst van het eerste streepje in de opmerkingen van de BIM-Commissie betreffende het nieuwe artikel 13/1/1 (p. 4), wordt in de vraag van het diensthoofd tevens de synthese opgenomen van de risicoanalyse met betrekking tot de betrouwbaarheid van de bron en de risico's waar zij zich aan blootstelt in het kader van het plegen van het strafbaar feit of de strafbare feiten. Deze omvat de beoordeling van diens persoonlijkheid, gerechtelijke antecedenten, motivering, …

De inhoud van de risicoanalyse en de samenvatting ervan zullen overigens nader worden omschreven bij de actualisering van de richtlijn van de Nationale Veiligheidsraad van 25 maart 2019.

Art. 13/1/1 § 3

Die strafbare feiten moeten noodzakelijkerwijs in verhouding staan tot het doel en moeten binnen het kader van de opdracht van de betrokken dienst vallen.

Pour répondre au point 2.3. de l'avis du Collège des procureurs généraux, il est précisé que la source ne peut agir que dans le cadre des missions des services de renseignement visées aux articles 7, 8 et 11 de la LRS et dans les limites du concours que la source apporte à ces missions.

Par ailleurs, le Collège des procureurs généraux fait une comparaison entre les enquêtes de renseignement et les enquêtes pénales qui n'a pas lieu d'être car les finalités des deux types de procédures sont totalement différentes comme expliqué ci-dessus (art. 13/1/1,§ 2).

Art. 13/1/1 § 4

La source doit signer un mémorandum contenant notamment les conditions de mise en œuvre de l'infraction autorisée et les modalités de rapportage.

Pour répondre au 1er tiret des remarques de la Commission BIM concernant le nouvel article 13/1/1 (p.4), ce mémorandum est transmis à la Commission qui doit à son tour le transmettre au Comité permanent R (voir les nouveaux paragraphes 4 et 8). Le mémorandum est conservé dans le dossier individuel de la source qui est conservé au sein du service concerné.

Pour tenir compte de la remarque 40 de l'avis du Comité R, le projet de loi est complété par les mentions obligatoires que ce mémorandum devra contenir, comme le code d'identification de la source, les droits et obligations de la source dans le cadre de la commission de l'infraction autorisée, les instructions et les conditions strictes dans le cadre desquelles l'infraction peut être commise, …

Ainsi, les droits et les obligations et les instructions incluent notamment l'interdiction de porter atteinte à l'intégrité physique d'une personne, les instructions en matière de discrétion, la période au cours de laquelle l'infraction peut être commise, …

Pour répondre au point 45 du Comité R, les conditions d'indemnisation en cas de dommage(s) à la source et/ou au(x) tiers seront également précisées dans le mémorandum (voir l'explication ci-dessous concernant l'article 13/1/1 § 11).

Pour répondre à la remarque 26 de l'avis du Comité R, la source humaine fera rapport à l'agent chargé du suivi du déroulement de l'infraction dès que possible, étant donné qu'il peut arriver que la source et/ou l'agent chargé du suivi du déroulement de l'infraction doivent

In antwoord op punt 2.3. van het advies van het College van procureurs-generaal wordt verduidelijkt dat de bron slechts mag handelen in het kader van de opdrachten van de inlichtingendiensten beschreven in de artikelen 7, 8 en 11 van de WIV en binnen de grenzen van de medewerking die de bron verleent aan deze opdrachten.

Het College van procureurs-generaal maakt overigens een vergelijking tussen inlichtingenonderzoeken en strafonderzoeken, die niet opgaat aangezien de doeleinden van beide soorten procedures totaal verschillend zijn, zoals hierboven werd uiteengezet (art. 13/1/1,§ 2).

Art. 13/1/1 § 4

De bron moet een memorandum ondertekenen met daarin onder meer de voorwaarden voor de uitvoering van het toegestane strafbare feit en de modaliteiten voor de verslaggeving.

In antwoord op de tekst van het eerste streepje in de opmerkingen van de BIM-Commissie betreffende het nieuwe artikel 13/1/1 wordt dit memorandum naar de Commissie gestuurd, die het op haar beurt naar het Vast Comité I moet doorsturen (zie de nieuwe paragrafen 4 en 8). Het memorandum wordt bewaard in het individuele dossier van de bron, dat binnen de betrokken dienst bewaard wordt.

Om rekening te houden met opmerking 40 in het advies van het Comité I wordt het wetsontwerp aangevuld met de verplichte vermeldingen die het memorandum moet bevatten, zoals de identificatiecode van de bron, de rechten en plichten van de bron in het kader van het plegen van het toegelaten strafbaar feit, de instructies en de strikte voorwaarden in het kader waarvan het strafbaar feit mag worden gepleegd, …

Zo houden de rechten en plichten en de instructies onder meer het verbod in om afbreuk te doen aan de fysieke integriteit van een persoon, de instructies op het stuk van discretie, de periode waarbinnen het strafbaar feit mag worden gepleegd, …

In antwoord op punt 45 van het Comité I kunnen de voorwaarden voor de schadeloosstelling in geval van schade aan de bron en aan een derde of derden ook toegevoegd worden in het memorandum (zie de uitleg hieronder met betrekking tot artikel 13/1/1 § 11).

In antwoord op opmerking 26 in het advies van het Comité I brengt de menselijke bron zo snel mogelijk verslag uit aan de agent belast met de opvolging van het verloop van het strafbaar feit, aangezien het kan gebeuren dat de bron en/of de agent belast met de

attendre un moment propice afin d'éviter tout risque pour leur sécurité (point 26 § 2 de l'avis du Comité R).

Art. 13/1/1 § 5

Dès que l'infraction a été commise, la source en informe l'agent chargé du suivi du déroulement de l'infraction du service de renseignement et de sécurité concerné qui en informe sa hiérarchie jusqu'au dirigeant du service. Ce dernier informe également la Commission.

Pour répondre au commentaire de la Commission BIM, (3e tiret pour l'art. 13/1/1, page 4), il n'est pas prévu que la Commission BIM soit informée dans les vingt-quatre heures suivant la commission de l'infraction étant donné que, comme expliqué ci-dessus, il ne sera pas toujours possible, pour des raisons de sécurité de la source et/ou de l'agent chargé du suivi, de faire rapport dans un délai si court. La transmission de l'information sera donc effectuée dans les plus brefs délais.

Si la mesure a été autorisée pour une période supérieure à deux semaines, le service de renseignement et de sécurité concerné fait rapport toutes les deux semaines.

Un alinéa est ajouté pour qu'à la demande motivée de la Commission, le rapport puisse lui être transmis à plus courte échéance, pour autant que l'agent et la source soient en sécurité pour le faire, tout en tenant compte des besoins opérationnels et en restant proportionnel.

Art. 13/1/1 § 6

Afin d'uniformiser la procédure d'extrême urgence dans toute cette section, celle prévue au paragraphe 6 de l'article 13/1 est également applicable au nouvel article 13/1/1 (au paragraphe 6).

Pour suivre l'avis du Comité R (point 47), le paragraphe 6 est adapté afin qu'il soit également conforme à la procédure d'extrême urgence en méthode exceptionnelle: "la Commission" a été remplacée par "le président ou le membre contacté" lors de la confirmation de son accord le plus rapidement possible.

Par ailleurs, deux conditions sont ajoutées: la procédure d'extrême urgence pour autoriser la source à commettre une infraction n'est possible que dans des circonstances exceptionnelles et lorsque la menace potentielle est grave.

opvolging van het verloop van het strafbaar feit een geschikt moment dienen af te wachten om elk risico voor hun veiligheid te vermijden (punt 26, § 2 van het advies van het Comité I).

Art. 13/1/1 § 5

Zodra het strafbaar feit is gepleegd, brengt de bron de betrokken agent van de inlichtingen- en veiligheidsdienst belast met de opvolging van het verloop van het strafbaar feit hiervan op de hoogte. Deze informeert op zijn beurt zijn hiërarchie tot en met het diensthoofd. Deze laatste brengt ook de Commissie op de hoogte.

In antwoord op de opmerking van de BIM-Commissie (3e streepje voor art. 13/1/1, pagina 4) is het niet voorzien dat de BIM-Commissie binnen de 24 uur na het plegen van het strafbaar feit op de hoogte wordt gebracht, aangezien het met het oog op de veiligheid van de bron en/of de agent belast met de opvolging, zoals hierboven uiteengezet, niet altijd mogelijk zal zijn om op zo'n korte termijn verslag uit te brengen. De informatie zal dus zo spoedig mogelijk worden overgemaakt.

Indien de maatregel toegestaan werd voor een periode van meer dan twee weken, brengt de betrokken inlichtingen- en veiligheidsdienst om de twee weken verslag uit.

Een lid wordt ingevoegd opdat, op gemotiveerd verzoek van de Commissie, het verslag haar op kortere termijn kan worden overgemaakt, voor zover de agent en de bron in veiligheid zijn en rekening houdend met de operationele noden en de proportionaliteit.

Art. 13/1/1 § 6

Teneinde de hoogdringendheidsprocedure in deze volledige afdeling te uniformeren, is de procedure waarin paragraaf 6 van artikel 13/1 voorziet ook toepasselijk op het nieuwe artikel 13/1/1 (paragraaf 6).

In navolging van het advies van het Comité I (punt 47) wordt paragraaf 6 aangepast, zodat deze in overeenstemming is met de procedure voorzien in geval van hoogdringendheid voor een uitzonderlijke methode: "de Commissie" werd vervangen door "de voorzitter of het gecontacteerde lid" voor de zo spoedig mogelijke bevestiging van zijn akkoord.

Twee voorwaarden worden overigens toegevoegd: de hoogdringendheidsprocedure voor de machtiging van een bron om een strafbaar feit te plegen is enkel mogelijk in uitzonderlijke omstandigheden en in geval van een ernstige potentiële dreiging.

Pour répondre à l'avis du Conseil d'État (article 6, point 3), les subdivisions de l'article 13/1/1 qui restent applicables à la source humaine dans la procédure d'extrême urgence sont ajoutées dans la loi.

Pour répondre à la Commission BIM (4e tiret des remarques de l'art. 13/1/1, p. 4), la procédure d'extrême urgence est maintenue car elle sera nécessaire, même si elle ne devrait normalement pas être appliquée fréquemment. Néanmoins, pour répondre aux craintes de la Commission BIM, il est précisé que l'analyse de risques ainsi que le mémorandum sont des préalables qui restent d'application même en cas d'extrême urgence.

Contrairement à ce qui est prévu pour l'agent des services de renseignement et de sécurité, la source n'a pas le droit de commettre des infractions pour lesquelles elle n'a pas reçu d'accord préalable et ainsi, aucune régularisation a posteriori en cas d'imprévisibilité n'est prévue pour les sources humaines.

Art. 13/1/1 § 7

Afin de tenir compte de la remarque du Comité R (point 34), les auteurs du projet insèrent un nouveau paragraphe 7 qui permet au service de renseignement concerné de saisir le Comité R lorsque la Commission BIM a rendu une décision négative ou n'a rendu aucune décision dans le délai légal. Le Comité R décide alors s'il autorise, ou non, l'infraction.

Pour répondre à l'avis de la Commission BIM (p.5, 1er tiret), les auteurs du projet précisent que ce n'est pas une nouvelle compétence du Comité R puisqu'il peut déjà, en vertu de l'article 43/6, révoquer la décision de la Commission BIM, dans le cadre des BIM. En l'espèce, les auteurs du projet reprennent une compétence similaire dans le cadre des articles 13/1 et 13/1/1 car à défaut, ils ne seraient applicables que pour les BIM. Or, les auteurs souhaitent également prévoir une sorte de double contrôle pour une décision aussi sensible que d'autoriser une infraction.

Art. 13/1/1 § 8

Il est précisé dans le nouveau paragraphe 8 que la Commission a l'obligation de transmettre sans délai tous les documents visés dans les nouveaux paragraphes 2 à 5 au Comité permanent R.

In antwoord op het advies van de Raad van State (artikel 6, punt 3) worden de onderverdelingen van artikel 13/1/1 die van toepassing blijven op de menselijke bron in de hoogdringendheidsprocedure ingevoegd in de wet.

In antwoord op de BIM-Commissie (4e streepje van de opmerkingen op art. 13/1/1, p.4) blijft de hoogdringendheidsprocedure behouden omdat deze noodzakelijk zal zijn, zelfs indien ze normaliter niet frequent zal moeten worden toegepast. Niettemin wordt, in antwoord op de bezorgdheden van de BIM-Commissie, verduidelijkt dat de risicoanalyse alsook het memorandum voorafgaande voorwaarden vormen die zelfs in geval van hoogdringendheid van toepassing blijven.

In tegenstelling tot waarin is voorzien voor agenten van de inlichtingen- en veiligheidsdiensten, hebben bronnen niet het recht om strafbare feiten te begaan waarvoor zij geen voorafgaand akkoord hebben gekregen. Voor de menselijke bronnen die een onvoorzien strafbaar feit plegen, is dan ook geen enkele regularisatie voorzien.

Art. 13/1/1 § 7

Om rekening te houden met de opmerking van het Comité I (punt 34) voegen de opstellers van het ontwerp een nieuwe paragraaf 7 in die de betrokken inlichtingendienst in staat stelt om het Comité I te vatten wanneer de BIM-Commissie een negatieve beslissing heeft uitgebracht of geen beslissing heeft uitgebracht binnen de wettelijke termijn. Het Comité I beslist dan of het strafbaar feit al dan niet toestaat.

In antwoord op het advies van de BIM-Commissie (p.5, 1ste streepje), benadrukken de opstellers van het ontwerp dat het niet om een nieuwe bevoegdheid van het Comité I gaat, aangezien het krachtens artikel 43/6 de beslissing van de BIM-Commissie reeds kan intrekken in het kader van BIM's. In casu hernemen de opstellers van het ontwerp deze bevoegdheid in het kader van de artikelen 13/1 en 13/1/1, aangezien deze regels bij ontbreken van deze vermelding enkel van toepassing zouden zijn op BIM's. De opstellers wensen echter ook een vorm van dubbele controle te voorzien voor een beslissing die zo gevoelig is als het machtigen van een strafbaar feit.

Art. 13/1/1 § 8

In de nieuwe paragraaf 8 wordt vermeld dat de Commissie verplicht is om alle documenten waarnaar in de nieuwe paragrafen 2 tot 5 wordt verwezen, onverwijld toe te zenden aan het Vast Comité I.

Ainsi, ce dernier pourra utilement exercer son contrôle.

Par ailleurs, le Comité permanent R peut exercer son pouvoir de contrôle général en application de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace et donc entendre toute personne qu'il estime nécessaire ou se faire transmettre tous les documents utiles.

Art. 13/1/1 § 9

Le nouveau paragraphe 9 prévoit l'obligation pour le dirigeant du service de renseignement et de sécurité concerné de mettre fin à la mesure dès que possible si l'absolue nécessité de commettre une infraction a cessé d'exister, si la mesure n'est plus utile pour atteindre l'objectif ou si une illégalité est établie. Le dirigeant du service informe la Commission de cette décision dans les meilleurs délais.

En outre, à la demande de la Commission ou du Comité permanent R, si une illégalité est constatée, le dirigeant du service met fin à la mesure prévue ou en cours dès que possible.

Cela répond dès lors à l'avis de la Commission BIM (5e tiret, page 4), celle-ci peut en effet exiger du dirigeant du service concerné de mettre fin à la mesure en cours ou planifiée dès que possible si les conditions légales prévues à l'article 13/1/1 ne sont plus réunies: si la Commission constate que la mesure n'est plus nécessaire pour assurer l'exécution optimale de la mission ou garantir leur propre sécurité ou celle de tiers, ou qu'elle ne respecte plus l'exigence de proportionnalité.

En ce qui concerne le succès de la mission, l'autorisation de commettre une infraction étant une mesure d'appui à une méthode et non une méthode en elle-même, les auteurs du texte considèrent que le dirigeant du service concerné est mieux placé pour apprécier l'opportunité de mettre fin à la mesure si elle n'est plus utile pour atteindre l'objectif poursuivi.

Pour répondre au point 23 de l'avis du Comité R, il est précisé au paragraphe 9 alinéa 2 que lorsque la Commission ou le Comité permanent R constate une illégalité, elle ou il en informe le dirigeant du service concerné qui met fin à la mesure en cours ou planifiée dès que possible.

Si l'infraction est commise dans le cadre d'une méthode de recueil de données et que l'infraction est irrégulière,

Zo kan die laatste zijn toezicht op nuttige wijze uitoefenen.

Bovendien heeft het Vast Comité I de bevoegdheid om een algemene controle uit te oefenen krachtens de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en het Coördinatieorgaan voor de dreigingsanalyse, en aldus elke persoon die het nodig acht kan horen of alle noodzakelijke documenten kan inzien.

Art. 13/1/1 § 9

De nieuwe paragraaf 9 voorziet in de verplichting voor het betrokken diensthoofd om de maatregel te beëindigen wanneer het niet meer absoluut noodzakelijk is om een strafbaar feit te plegen, wanneer de maatregel niet langer nuttig is voor het te bereiken doel of wanneer een onwettigheid wordt vastgesteld. Het diensthoofd brengt deze beslissing zo spoedig mogelijk ter kennis van de Commissie.

Indien er een onwettigheid wordt vastgesteld, wordt een geplande of lopende maatregel bovendien zo spoedig mogelijk beëindigd door het diensthoofd, op verzoek van de Commissie of het Vast Comité I.

Dit beantwoordt bijgevolg aan het advies van de BIM-Commissie (5e streepje, p.4). Deze laatste kan immers van het diensthoofd eisen dat hij de geplande of lopende maatregel zo snel mogelijk beëindigt indien de wettelijke voorwaarden bedoeld in artikel 13/1/1 niet meer vervuld zijn: indien de Commissie vaststelt dat de maatregel niet langer nodig is om het welslagen van de opdracht de verzekeren of de eigen veiligheid of die van derden te vrijwaren, of als de maatregel niet langer niet langer voldoet aan de evenredigheidsvereiste.

Wat betreft het welslagen van de opdracht, beschouwen de opstellers van de tekst, aangezien de machtiging tot het plegen van een strafbaar feit een ondersteuningsmaatregel voor een methode is en geen methode op zich, dat het betrokken diensthoofd het best geplaatst is om te beoordelen wanneer het gepast is om de maatregel te beëindigen indien deze niet langer nuttig is om het nagestreefde doel te bereiken.

In antwoord op punt 23 van het advies van het Comité I wordt in paragraaf 9, lid 2 verduidelijkt dat wanneer de Commissie of het Vast Comité I een onwettigheid vaststellen, zij het betrokken diensthoofd hiervan op de hoogte brengen, dat de geplande of lopende maatregel zo snel mogelijk beëindigt.

Indien het strafbaar feit gepleegd wordt in het kader van een methode voor het verzamelen van gegevens en

la régularité de la méthode elle-même doit bien entendu être réévaluée.

Art. 13/1/1 § 10

Pour répondre aux points 25 et 26 du Comité R et aux préoccupations de la Commission BIM concernant l'accès au dossier de la source pour exercer leur contrôle, un paragraphe 10 est inséré.

Le contrôle de la Commission BIM s'étend sur les éléments suivants:

Un dossier papier sera réalisé. Dans ce dossier, seront mis à la disposition de la Commission BIM, dans les locaux des services de renseignement:

— Les extraits de la "proposition source", du projet d'approche et du projet de recrutement portant sur l'évaluation de la source et de son environnement, à l'exception des informations sur les modalités de protection de la source, de communication avec la source, de paiement de la source qui ne seront pas mis à disposition car elles ne sont pas pertinentes pour autoriser l'infraction;

— Toutes les évaluations réalisées par les agents chargés du suivi du déroulement de l'infraction;

— Durant la période d'autorisation de la commission d'infractions, l'agent chargé du suivi du déroulement de l'infraction devra rédiger après chaque contact avec sa source ayant un lien avec l'infraction une note-type qui donnera un suivi de la relation avec la source et des infractions commises, l'état d'esprit de la source (craintes, respect des consignes, relations et interactions avec les cibles, …).

Les compétences de la Commission BIM dans le cadre d'une méthode exceptionnelle visée à l'article 18/10 § 6 ont été en grande partie reprises mais adaptées à la situation: si les auteurs du projet ont voulu garder le même niveau de protection juridique que pour une méthode exceptionnelle, la procédure doit néanmoins être adaptée: il n'est en effet pas possible d'appliquer *mutatis mutandis* les mêmes compétences, comme par exemple, aller sur les lieux de l'infraction pour contrôler la légalité de la mesure.

Par contre, la Commission pourra entendre l'agent chargé du suivi du déroulement de l'infraction, en présence de son supérieur hiérarchique, ce supérieur

het strafbaar feit onwettig is, moet de regelmatigheid van de methode zelf uiteraard opnieuw beoordeeld worden.

Art. 13/1/1 § 10

In antwoord op de punten 25 en 26 van het Comité I en op de bezorgdheden van de BIM-Commissie betreffende de toegang tot het dossier van de bron om hun toezicht uit te oefenen, wordt een paragraaf 10 ingevoegd.

Het toezicht van de BIM-Commissie omvat de volgende elementen:

Een papieren dossier zal worden gemaakt. In dit dossier worden volgende zaken ter beschikking gesteld van de BIM-Commissie in de lokalen van de inlichtingendiensten:

— de uittreksels uit het 'bronvoorstel' van het benaderingsontwerp en het rekruteringsontwerp die betrekking hebben op de beoordeling van de bron en diens omgeving, met uitzondering van de informatie over de modaliteiten voor de bescherming van de bron, de communicatie met de bron en de betaling van de bron, die niet ter beschikking wordt gesteld omdat ze informatie niet relevant is voor de machtiging van het strafbaar feit;

— alle uitgevoerde beoordelingen door de agenten belast met de opvolging van het verloop van het strafbaar feit:

— tijdens de periode waarin het plegen van het strafbaar feit is toegelaten, moet de agent belast met de opvolging van het verloop van het strafbaar feit na elk contact met zijn bron die verbonden is aan het strafbaar feit een standaardnota opstellen die een opvolging van de relatie met de bron, de gepleegde strafbare feiten, de houding van de bron (bezorgdheden, naleving van instructies, relaties en interacties met de doelwitten, enz.) mogelijk maakt.

De bevoegdheden van de BIM-Commissie in het kader van een uitzonderlijke methode bedoeld in artikel 18/10 § 6 werden dus grotendeels hernomen, maar aangepast aan de situatie: hoewel de auteurs van het ontwerp hetzelfde niveau van juridische bescherming hebben willen behouden als voor een uitzonderlijke methode, moet de procedure niettemin worden aangepast: het is immers niet mogelijk om dezelfde bevoegdheden, bijvoorbeeld naar de plaats van het strafbaar feit gaan om de wettelijkheid van de maatregel te controleren, *mutatis mutandis* toe te passen.

hiérarchique et tout autre responsable de la gestion de ladite source.

Pour répondre au point 39 de l'avis du Comité R, les auteurs du projet souhaitent réitérer l'importance pour un service de renseignement de protéger l'identité de ses sources. Raison pour laquelle l'accès aux noms de celles-ci est extrêmement limité, même au sein du service de renseignement.

Ainsi, le dossier papier contiendra le code d'identification de la source et non son identité. Si un contrôle du nom de la source est nécessaire, seul le Comité R y aura accès, et ce dans les installations du service concerné.

Art. 13/1/1 § 11

Comme indiqué dans les avis du Comité R (point 45) et du Conseil d'État (article 6, point 4), les modalités de l'indemnisation du dommage causé à un tiers ou subi par la source, lorsque celle-ci est autorisée à commettre une infraction, seront déterminées dans le mémorandum visé au paragraphe 4 de l'article 13/1/1.

Ainsi, en ce qui concerne les dommages que la source pourrait elle-même subir dans le cadre de l'exécution conforme de sa mission, une assurance sera contractée auprès d'une compagnie d'assurance pour couvrir les éventuels préjudices subis.

Pour ce qui concerne l'indemnisation aux tiers, victimes d'un dommage suite à la commission de l'infraction par la source, la question étant également pertinente pour les infiltrants civils en matière judiciaire (art. 47novies/1, /2 et /3), les auteurs du projet souhaitent poursuivre la réflexion avec les autorités judiciaires afin de mettre en place un système similaire.

Par conséquent, les auteurs du projet ont préféré supprimer le nouveau paragraphe 11 qui n'apporte aucune plus-value et qui, comme relevé par l'avis du Collège des Procureurs généraux (point 2.4), est, comme tel, incomplet.

Art. 8

Un nouvel article 13/1/2 est introduit par souci de clarté.

De Commissie kan daarentegen de agent belast met de opvolging van het verloop van het strafbaar feit horen, in het bijzijn van zijn hiërarchische meerdere, alsook deze hiërarchische meerdere en ieder ander die verantwoordelijk is voor de behandeling van voornoemde bron.

In antwoord op punt 39 van het advies van het Comité I wensen de auteurs van het ontwerp het belang voor een inlichtingendienst om zijn bronnen te beschermen, nogmaals te benadrukken. Om die reden is de toegang tot de namen van bronnen uiterst beperkt, zelfs binnen de inlichtingendienst zelf.

Zo zal de het papieren dossier niet de identiteit van de bron bevatten, maar zijn identificatiecode. Indien een controle van de naam van de bron noodzakelijk is, heeft enkel het Comité I er toegang toe en dit binnen de vestigingen van de betrokken dienst.

Art. 13/1/1 § 11

Zoals aangegeven in het advies van het Comité I (punt 45) en van de Raad van State (artikel 6, punt 4) worden de modaliteiten van schadeloosstelling ingeval van schade veroorzaakt aan een derde of geleden door de bron, vastgelegd in het memorandum bedoeld in paragraaf 4 van artikel 13/1/1.

Zo wordt er, in verband met de schade die de bron zelf zou lijden in het kader van de correcte uitoefening van haar opdracht, een verzekering gesloten bij een verzekeringsmaatschappij om de eventueel geleden schade te dekken.

De kwestie van de schadeloosstelling van derden, die schade kunnen lijden doordat de bron een strafbaar feit pleegt, was eveneens aan de orde bij de burgerinfiltratie in gerechtelijke zaken (art. 47novies/1, /2 en /3. Daarom wensen de auteurs van dit ontwerp de gedachtewisseling met de gerechtelijke overheden verder te zetten, om tot een gelijkaardig systeem te komen.

Bijgevolg hebben de opsteller van het ontwerp ervoor gekozen om de nieuwe paragraaf 11 weg te laten, omdat die geen enkele meerwaarde biedt en op zich onvolledig is, zoals werd aangegeven door het advies van het College van procureurs-generaal (punt 2.4).

Art. 8

Er wordt een nieuw artikel 13/1/2 ingevoegd voor meer duidelijkheid.

Art. 13/1/2, § 1er

Il est précisé que la Commission fonctionne selon toutes les modalités visées à l'article 43/1.

Art. 13/1/2, § 2 à § 4

L'exemption de peine dans le cas où un agent ou une source commet une infraction est étendue aux agents chargés du suivi du déroulement de l'infraction qui supervisent ou contrôlent les sources humaines, aux supérieurs hiérarchiques ainsi qu'aux magistrats de la Commission qui autorisent à commettre l'infraction et aux membres du Comité permanent R et du service d'enquête.

Pour répondre au point 41 de l'avis du Comité R, l'exemption de peine pour les membres du Comité R est maintenue étant donné que celui-ci pourrait avoir un rôle actif dans l'autorisation de commettre une infraction dans l'hypothèse où le Comité R est saisi suite à un avis négatif de la Commission BIM ou à l'absence d'avis de celle-ci rendu dans le délai légal (articles 13/1 § 8 et 13/1/1 § 7).

Art. 9

Le chapitre 3, section 2, est subdivisé en 4 sous-sections afin d'établir une distinction claire entre les différentes mesures de protection et d'appui.

L'article 9 insère une sous-section 2 qui comprend les dispositions relatives à l'utilisation d'un faux nom et d'une fausse qualité et à l'utilisation d'une identité et d'une qualité fictives.

Art. 10

L'article 13/2 détermine les règles applicables à la création et l'utilisation d'un faux nom, d'une fausse qualité, d'une identité fictive et d'une qualité fictive pour des raisons de sécurité liées à la protection des agents ou de tiers.

Ces règles s'appliquent dans toutes les hypothèses où cette protection est nécessaire:

— l'utilisation d'un faux nom, d'une fausse qualité ou d'une identité et/ou qualité fictive pour effectuer, en toute discrétion, dans le cadre de son travail, des actes tels que: acheter du matériel en toute discrétion (acheter une carte SIM prépayée ou du matériel technique avec une

Art. 13/1/2, § 1

Er wordt verduidelijkt dat de Commissie volgens alle modaliteiten bedoeld in artikel 43/1 functioneert.

Art. 13/1/2, § 2 tot § 4

De vrijstelling van straf wanneer een agent of een bron een strafbaar feit begaat, wordt uitgebreid tot de agenten belast met de opvolging van het verloop van het strafbaar feit die de menselijke bronnen begeleiden of controleren, de hiërarchische oversten en de magistraten van de Commissie die machtiging verlenen om het strafbaar feit te plegen en aan de leden van het Vast Comité I en de enquêtedienst.

In antwoord op punt 41 van het advies van het Comité I, blijft de vrijstelling van straf behouden voor de leden van het Comité I, aangezien deze een actieve rol kunnen spelen bij de machtiging voor het plegen van een strafbaar feit ingeval het Comité I gevat wordt na een negatief advies van de BIM-Commissie of bij gebrek aan een advies binnen de wettelijke termijn (artikelen 13/1 § 8 en 13/1/1 § 7).

Art. 9

Hoofdstuk 3, afdeling 2 wordt onderverdeeld in 4 onderafdelingen zodat er een duidelijk onderscheid bestaat tussen de verschillende beschermings- en ondersteuningsmaatregelen.

Artikel 9 voegt een onderafdeling 2 in die de bepalingen omvat over het gebruik van een valse naam en een valse hoedanigheid en de inzet van een fictieve identiteit en hoedanigheid.

Art. 10

Artikel 13/2 voorziet in de mogelijkheid om een valse naam, een valse hoedanigheid, een fictieve identiteit en een fictieve hoedanigheid te creëren en te gebruiken voor veiligheidsredenen verbonden aan de bescherming van agenten of derden.

Deze regels zijn van toepassing in alle hypotheses waar deze bescherming nodig is:

— Het gebruik van een valse naam, een valse hoedanigheid of een fictieve identiteit en/of hoedanigheid, om in alle discretie, binnen het kader van het werk, daden te kunnen stellen zoals: het aankopen in alle discretie van materieel (kopen van een prepaid simkaart of technisch

identité fictive, …), louer un appartement sans exposer le nom de famille de l'agent,…etc.;

— la même utilisation pour protéger un agent dans le cadre de la mise en œuvre d'une méthode de recueil de données;

— cette même utilisation pour protéger l'agent qui fait une rencontre fortuite et potentiellement dangereuse;

— Etc.

D'autres modalités pratiques de mise en œuvre sont en outre prévues à l'article 2 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.

L'utilisation d'un faux nom, d'une fausse qualité, d'une identité fictive ou d'une qualité fictive est une mesure de protection et d'appui, comme le précise l'intitulé de la section 2 du chapitre III de la LRS dont l'article 13/2 fait partie. Ce n'est donc pas, en soi, une méthode de recueil de données.

Ceci étant, si des raisons de sécurité le justifient, un agent mettant en œuvre une méthode de recueil de données peut recourir à un faux nom ou une identité fictive pour se protéger.

De même, lorsque, par exemple, un achat de matériel nécessite une discrétion absolue, l'agent utilisant une identité fictive peut prendre des informations sur le prix du matériel, le délai de livraison, …

À l'article 13/2, alinéa 3, le mot "temporaire" est supprimé car c'est un concept imprécis qui n'apporte aucune plus-value à cet article. Au contraire, dans la pratique, il prête plus à confusion qu'il n'apporte une précision utile.

Il est d'ailleurs tout à fait possible qu'une identité fictive soit utilisée pendant une longue période, par exemple, dans le cadre d'une surveillance sur internet.

Art. 11

Le chapitre 3, section 2, est subdivisé en 4 sous-sections afin d'établir une distinction claire entre les différentes mesures de protection et d'appui.

materieel met een fictieve identiteit, …), een appartement huren zonder de familienaam van de agent bloot te geven, etc.;

— Hetzelfde gebruik om een agent te beschermen bij de aanwending van een methode voor het verzamelen van gegevens;

— Hetzelfde gebruik om een agent te beschermen die een toevallige en potentieel gevaarlijke ontmoeting heeft;

— Enz.

Andere praktische modaliteiten bij de aanwending zijn ook opgenomen in artikel 2 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.

Het gebruik van een valse naam, een valse hoedanigheid, een fictieve identiteit of hoedanigheid is een beschermings- en ondersteuningsmaatregel, zoals de titel van afdeling 2 van hoofdstuk III van de WIV waarvan artikel 13/2 deel uitmaakt, aangeeft. Het is dus niet een methode voor het verzamelen van gegevens op zich.

Indien gerechtvaardigd omwille van veiligheidsredenen, mag een agent die een methode voor het verzamelen van gegevens aanwendt gebruik maken van een valse naam of een fictieve identiteit om zich te beschermen.

Hetzelfde geldt wanneer bijvoorbeeld de aankoop van materieel een absolute discretie vereist; dan mag de agent die een fictieve identiteit gebruikt informatie inwinnen over de prijs van het materieel, de leveringstermijn, ….

In het artikel 13/2, derde lid wordt het woord "tijdelijk" geschrapt omdat het een onduidelijk begrip is dat geen meerwaarde toevoegt aan dit artikel. Integendeel, in de praktijk leidt het eerder tot verwarring dan dat het een nuttige opheldering verschaft.

Het is overigens best mogelijk dat een fictieve identiteit voor een lange periode gebruikt wordt, bijvoorbeeld in het kader van een online surveillance.

Art. 11

Hoofdstuk 3, afdeling 2 wordt onderverdeeld in 4 onderafdelingen zodat er een duidelijk onderscheid bestaat tussen de verschillende beschermings- en ondersteuningsmaatregelen.

L'article 11 insère une sous-section 3 qui comprend la disposition 13/3 relative à la création et à l'utilisation de personnes morales.

Art. 12

Le chapitre 3, section 2, est subdivisé en 4 sous-sections afin d'établir une distinction claire entre les différentes mesures de protection et d'appui.

L'article 12 insère une sous-section 4 qui comprend la disposition 13/4 relative à la coopération avec des tiers.

Art. 13

L'article 13/4 concerne l'aide que des tiers peuvent apporter aux services de renseignement et de sécurité. On entend par "tiers" principalement des partenaires étrangers ou des experts prêtant leur assistance technique et non les sources humaines qui sont, elles, visées à l'article 18. A titre d'exemples, le tiers peut être un serrurier qui aide à pénétrer discrètement dans un lieu fermé ou un traducteur-interprète. L'aide apportée se fait toujours sous le contrôle du service de renseignement concerné, qui reste maître de l'opération.

La loi prévoit déjà une cause d'excuse absolutoire pour les contraventions, les infractions au code de la route ou les vols d'usage (article 13/1 alinéa 2) ou lorsqu'ils commettent une infraction, dans le cadre de leur assistance à l'exécution d'une méthode spécifique ou exceptionnelles (article 13/1 alinéa 3).

Les infractions imprévisibles régularisées a posteriori ne sont pas possibles. Faire appel à un tiers doit être préparé et la possibilité qu'il commette une infraction doit aussi être anticipée.

Par contre, rien n'est prévu pour les tiers qui apportent leur assistance en dehors de ces deux hypothèses limitées.

Les modifications apportées permettent de couvrir toutes les hypothèses où le tiers apporte son aide aux services de renseignement et de sécurité, en application de la présente loi.

Les infractions imprévisibles régularisées *a posteriori* restent exclues du champ d'application.

Artikel 11 voegt een onderafdeling 3 in die de bepaling 13/3 omvat over de oprichting en inzet van rechtspersonen.

Art. 12

Hoofdstuk 3, afdeling 2 wordt onderverdeeld in 4 onderafdelingen zodat er een duidelijk onderscheid bestaat tussen de verschillende beschermings- en ondersteuningsmaatregelen.

Artikel 12 voegt een onderafdeling 4 in die de bepaling 13/4 omvat over de medewerking van derden.

Art. 13

Het artikel 13/4 betreft de hulp die derden de inlichtingen- en veiligheidsdiensten kunnen bieden. Onder "derden" worden voornamelijk buitenlandse partners of deskundigen die technische bijstand verlenen, verstaan en niet de menselijke bronnen die in artikel 18 worden beoogd. Zo kan bijvoorbeeld een slotenmaker die hulp biedt om discreet binnen te dringen in een gesloten plaats een derde zijn, of een vertaler-tolk. De hulp wordt altijd geleverd onder de controle van de betrokken inlichtingendienst, die baas blijft over de operatie.

De wet voorziet reeds in een strafuitsluitende verschoningsgrond voor overtredingen, inbreuken op de wegcode of gebruiksdiefstallen (artikel 13/1, tweede lid) of voor strafbare feiten gepleegd in het kader van bijstand bij de uitvoering van een specifieke of uitzonderlijke methode (artikel 13/1, derde lid).

Onvoorzienbare strafbare feiten kunnen niet a posteriori worden geregulariseerd. Wanneer een beroep wordt gedaan op een derde, moet dat worden voorbereid en er moet ook worden geanticipeerd op de mogelijkheid dat die derde een strafbaar feit begaat.

Er is daarentegen in niets voorzien voor de derden die bijstand verlenen buiten het kader van deze twee beperkte hypothesen.

De aangebrachte wijzigingen beschermen ook alle situaties waarbij de derde zijn hulp verleent aan de inlichtingen- en veiligheidsdiensten, bij toepassing van deze wet.

Het *a posteriori* regulariseren van onvoorzienbare strafbare feiten wordt niet in het toepassingsgebied opgenomen.

Les nouveaux paragraphes 2 à 5 et 7 à 9 de l'article 13/1 sont rendus applicables à l'article 13/4.

Art. 14

L'article 14 concerne l'article 16/3 de la LRS, introduit par la loi du 25 décembre 2016 relative au traitement des données des passagers (*Moniteur belge* du 25/01/2017). Cet article 16/3 régit l'accès par les services de renseignement aux données sur les passagers dont la collecte systématique et la conservation dans une banque de données centrale est prévue par cette loi du 25 décembre 2016.

L'article 14 apporte les modifications suivantes:

Tout d'abord (article 2 du présent projet de loi), il permet au dirigeant du service de désigner un délégué habilité à décider, comme le dirigeant du service, la méthode visée à l'article 16/3 et donc l'accès aux données sur les passagers.

Cette modification est cohérente avec les articles 16/2 et 16/4 de la LRS qui font aussi expressément référence au délégué lors d'une réquisition en matière de communications électroniques et lors de certains accès aux données collectées au moyen de caméras utilisées par les services de police. Pour un meilleur fonctionnement interne de la charge de travail, il est nécessaire que le dirigeant du service puisse déléguer cette tâche, si nécessaire, à quelqu'un d'autre pour faire le suivi de certaines méthodes ordinaires.

La deuxième modification apportée à l'article 16/3 concerne l'ajout d'une procédure d'urgence dans laquelle la décision d'accéder aux données sur les passagers est prise oralement dans un premier temps. Une telle autorisation verbale est prévue pour toutes les autres méthodes de recueil de données. A titre d'exemple, l'article 16/2 § 1er, al.2 (en matière de communications électroniques) de la LRS prévoit: "En cas d'urgence, le dirigeant de service ou son délégué peut requérir ces données verbalement. Cette réquisition verbale est confirmée dans un délai de vingt-quatre heures par une réquisition écrite."

Par ailleurs, pour uniformiser les procédures d'extrême urgence, les auteurs du projet ont repris la formulation applicable pour les méthodes spécifiques, c'est-à-dire, que la décision verbale est confirmée par une décision écrite, le premier jour ouvrable qui suit la date de la décision (voir article 18/3 § 3 LRS).

De nieuwe paragrafen 2 tot 5 en 7 tot 9 van artikel 13/1 zijn van toepassing gemaakt op artikel 13/4.

Art. 14

Artikel 14 heeft betrekking op artikel 16/3 van de WIV, ingevoegd bij de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens (BS 25 januari 2017). Dit artikel 16/3 regelt de toegang van de inlichtingendiensten tot de passagiersgegevens waarvan de stelselmatige verzameling en bewaring in een centrale gegevensbank is bepaald bij de wet van 25 december 2016.

Artikel 14 brengt de volgende wijzigingen aan:

Ten eerste biedt (artikel 2 van dit wetsontwerp) het diensthoofd de mogelijkheid een gedelegeerde aan te wijzen die, net zoals het diensthoofd, gemachtigd is om te besluiten tot de in artikel 16/3 bedoelde methode en dus tot de toegang tot de passagiersgegevens.

Die wijziging strookt met de artikelen 16/2 en 16/4 van de WIV, waarin ook uitdrukkelijk wordt verwezen naar de gedelegeerde bij een vordering inzake elektronische communicatiediensten en bij sommige toegangen tot gegevens die verzameld worden door middel van camera's die door de politiediensten worden gebruikt. Voor een betere interne verdeling van de werklast is het noodzakelijk dat het diensthoofd deze taak indien nodig aan iemand anders kan delegeren om sommige gewone methoden op te volgen.

De tweede wijziging aangebracht in artikel 16/3 betreft de toevoeging van een spoedprocedure waarbij de beslissing om toegang te hebben tot de passagiersgegevens in eerste instantie mondeling wordt genomen. In een dergelijke mondelinge machtiging is voorzien voor alle andere methoden voor het verzamelen van gegevens. Zo is in artikel 16/2, § 1, tweede lid, (inzake elektronische communicatie) van de WIV het volgende bepaald: "In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde deze gegevens mondeling vorderen. Deze mondelinge vordering wordt binnen vierentwintig uur bevestigd door een schriftelijke vordering."

Verder, om de procedures voor hoogdringendheid gelijkvormig te maken, hebben de opstellers van het ontwerp overigens de verwoording hernomen die van toepassing is op de specifieke methoden, namelijk: de mondelinge beslissing wordt de eerste werkdag volgend op de datum van de beslissing bevestigd door een schriftelijke beslissing (zie artikel 18/3 § 3 WIV).

En outre, une telle procédure est essentielle pour le bon fonctionnement du service, qui est susceptible de mettre en œuvre des méthodes dans l'urgence, lorsque la menace est imminente.

La troisième modification est une simple correction technique suite à une erreur de formulation et ne modifie pas la portée de cet article.

Art. 15

L'article 15 concerne l'article 16/4 de la LRS, introduit par la loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière (*Moniteur belge* du 16/04/2018). Cet article 16/4 régit l'accès des services de renseignement aux données collectées par des caméras utilisées par les services de police.

Pour tenir compte du point 8 de l'avis du Comité R, le concept d' "officier de renseignement" est remplacé aux paragraphes 2, 3 et 6 par l' "officier des méthodes" afin de faire correspondre le titre de cet agent avec l'évolution de ses compétences (voir article 2 du présent projet de loi);

La modification apportée à l'article 16/4 concerne l'ajout d'une procédure d'urgence dans laquelle la décision d'accéder aux données collectées par des caméras utilisées par les services de police est prise oralement dans un premier temps. Une telle autorisation verbale est prévue pour toutes les autres méthodes de recueil de données. Comme pour l'article 16/3, il s'agit de combler une lacune par rapport à l'article 16/2 § 1er, al.2 de la LRS (en matière de communications électroniques), lequel prévoit: "*En cas d'urgence, le dirigeant de service ou son délégué peut requérir ces données verbalement. Cette réquisition verbale est confirmée dans un délai de vingt-quatre heures par une réquisition écrite*."

Par ailleurs, pour uniformiser les procédures d'extrême urgence, les auteurs du projet ont repris la formulation applicable pour les méthodes spécifiques, c'est-à-dire, que la décision verbale est confirmée par une décision écrite, le premier jour ouvrable qui suit la date de la décision (voir article 18/3 § 3 LRS).

Bovendien is een dergelijke procedure essentieel voor de goede werking van de dienst die vaak in hoogdringendheid methoden moet aanwenden wanneer er een onmiddellijke dreiging is.

De derde wijziging, is een louter technische verbetering van een foute formulering en wijzigt de draagwijdte van dit artikel niet.

Art. 15

Artikel 15 heeft betrekking op artikel 16/4 van de WIV, ingevoegd bij de wet van 21 maart 2018 tot wijziging van de wet op het politieambt teneinde 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 et 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 (B.S. 16/04/2018). Dit artikel 16/4 regelt de toegang van de inlichtingendiensten tot gegevens die verzameld worden door camera's die door de politiediensten worden gebruikt.

Om rekening te houden met punt 8 van het advies van het Comité I wordt het begrip "inlichtingenofficier" in de paragrafen 2, 3 en 6 vervangen door "methodenofficier", zodat de titel van deze agent overeenstemt met de evolutie van zijn bevoegdheden (zie artikel 2 van het huidige wetsontwerp);

De wijziging aangebracht in artikel 16/4 betreft de toevoeging van een spoedprocedure waarbij de beslissing om toegang te hebben tot de gegevens die verzameld worden door camera's die door de politiediensten worden gebruikt, in eerste instantie mondeling wordt genomen. En dergelijke mondelinge machtiging is voorzien voor alle andere methoden voor het inzamelen van gegevens. Zoals voor artikel 16/3 gaat het om het wegwerken van een leemte ten opzichte van artikel 16/2, § 1, tweede lid, van de WIV (inzake elektronische communicatie), dat het volgende bepaalt: "*In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde deze gegevens mondeling vorderen. Deze mondelinge vordering wordt binnen vierentwintig uur bevestigd door een schriftelijke vordering.*"

Verder, om de hoogdringendheidsprocedures uniform te maken, hebben de auteurs van het ontwerp de verwoording van toepassing op de specifieke methoden hernomen, namelijk: de mondelinge beslissing wordt bevestigd door een schriftelijke beslissing de eerste werkdag volgend op de datum van de beslissing (zie artikel 18/3 § 3 WIV).

Les modifications apportées au paragraphe 2, alinéa 4 et au paragraphe 3, alinéa 3 sont des simples corrections techniques suite à une erreur de formulation et ne modifie pas la portée de cet article.

En outre, une telle procédure est essentielle pour le bon fonctionnement du service, qui est susceptible de mettre en œuvre des méthodes dans l'urgence, lorsque la menace est imminente.

Art. 16

Un nouvel article 16/5 est inséré au chapitre 3, section 4, sous-section 1, concernant les méthodes ordinaires de collecte de données. Ce nouvel article vise à conférer aux services de renseignement et de sécurité une base légale plus solide leur permettant de s'infiltrer dans le monde virtuel sous couvert ou non d'un faux nom ou d'une fausse qualité.

Depuis plusieurs années, des agents des deux services de renseignement sont présents sur internet et essayent de s'infiltrer dans des milieux extrémistes, djihadistes, anarchistes ou autres afin de collecter des informations sur les menaces potentielles contre la sécurité nationale. Il n'est de secret pour personne que, par exemple, le recrutement et la propagande de l'État islamique passe par ce vecteur qu'est internet. La présence des services de renseignement y est donc indispensable.

Pour pouvoir collecter des données en toute discrétion, les agents peuvent utiliser des pseudonymes, des faux noms ou des fausses qualités. Cette méthode ordinaire de collecte d'informations dans le monde virtuel se fonde sur la compétence de collecte générale d'information par le biais de sources ouvertes, de contacts personnels et par analogie avec des observations dans le monde réel.

Dans le souci de clarifier la base légale lorsque les agents souhaitent, dans le monde virtuel, s'infiltrer de manière active dans un groupe ou dans la vie d'une personne faisant l'objet d'une enquête d'un service de renseignement et de sécurité, il a été jugé opportun d'ajouter un nouvel article dans la LRS.

Le nouvel article 16/5 vise donc à réglementer l'infiltration dans le monde virtuel sous couvert ou non d'un faux nom ou d'une fausse qualité mais sans identité ou qualité fictive.

Une définition de l'infiltration a été insérée à l'article 3, 27°. On entend dès lors par s'infiltrer:

De wijzigingen in paragraaf 2, vierde lid, en in paragraaf 3, derde lid, zijn louter technische verbeteringen van een foutieve verwoording en wijzigen de draagwijdte van dit artikel niet.

Bovendien is een dergelijke procedure essentieel voor de goede werking van de dienst die vaak in hoogdringendheid methoden moet aanwenden wanneer er een onmiddellijke dreiging is.

Art. 16

In Hoofdstuk 3, afdeling 4, onderafdeling 1 dat over de gewone methoden voor het verzamelen van gegevens gaat, wordt een nieuw artikel 16/5 toegevoegd. Dit nieuwe artikel dient om de inlichtingen- en veiligheidsdiensten een solidere wettelijke basis te geven, die hun toelaat in de virtuele wereld te infiltreren al dan niet met een valse naam of een valse hoedanigheid.

Al meerdere jaren zijn agenten van beide inlichtingendiensten aanwezig op het internet. Zij proberen te infiltreren in extremistische, jihadistische, anarchistische en andere milieus om informatie te verzamelen over mogelijke dreigingen tegen de nationale veiligheid. Het is algemeen bekend dat bijvoorbeeld Islamitische Staat het internet gebruikt voor werving en propaganda. Het is dus absoluut noodzakelijk dat de inlichtingendiensten aanwezig zijn op het internet.

Om in alle discretie gegevens te kunnen verzamelen, maken de agenten vaak gebruik van pseudoniemen, valse namen of valse hoedanigheden. Deze gewone methode om informatie in te zamelen in de virtuele wereld is gebaseerd op de algemene bevoegdheid van de inlichtingendiensten om informatie in te winnen via open bronnen, persoonlijke contacten en naar analogie met de observaties in de echte wereld.

Om duidelijkheid te verschaffen over de wettelijke basis wanneer agenten, in de virtuele wereld, op actieve wijze willen infiltreren in een groep of in het leven van een persoon die het voorwerp uitmaakt van een onderzoek van een inlichtingen- en veiligheidsdienst, werd het opportuun geacht om een nieuw artikel toe te voegen aan de WIV.

Het nieuwe artikel 16/5 beoogt dus een regeling voor de infiltratie in de virtuele wereld al dan niet met een valse identiteit of een valse hoedanigheid.

Een definitie van infiltratie werd ingevoegd in artikel 3, 27°. Onder infiltreren wordt dus begrepen:

"*le fait pour un agent, en dehors des cas visés à l'article 18, de s'intégrer délibérément dans un groupe ou dans la vie d'une personne afin de recueillir des informations ou des données, dans le cadre d'une enquête d'un service de renseignement et de sécurité et dans l'intérêt de l'exercice de ses missions, soit dans le monde virtuel, soit dans le monde réel. Cet agent dissimule sa qualité d'agent des services de renseignement et de sécurité, et pour les agents du Service Général du Renseignement et de la Sécurité, de membre du ministère de la Défense, et:*

a) participe ou facilite les activités ou soutient activement les convictions ou les activités de la personne ou du groupe qui fait l'objet de l'enquête, ou

b) entretient des relations durables avec ceux-ci.".

L'article 16/5 ne couvre pas les cas où l'Internet est utilisé par des agents et des sources pour communiquer entre eux (par courrier électronique, par exemple). Il ne s'agit pas d'infiltration, mais de contacts réguliers entre deux partenaires. L'article 18 continue dès lors de s'appliquer à ces contacts-là.

Aussi, il est précisé que l'observation sur internet en sources ouvertes (art. 13) avec l'utilisation d'une mesure d'appui déjà autorisée (art. 13/2) ne nécessite pas une nouvelle réglementation.

De manière générale, lorsque les conditions prévues dans la définition de l'infiltration ne sont pas réunies, la collecte d'informations dans le monde virtuel se fonde sur la compétence de collecte générale d'informations par le biais de sources ouvertes, de contacts personnels et par analogie avec des observations dans le monde réel.

Comme cette méthode est le 'pendant virtuel' des articles 16/1 et 17 L.R&S qui sont deux méthodes ordinaires, les auteurs du projet ont logiquement choisi d'en faire également une méthode ordinaire. Ce qui est visé ici, dans l'infiltration dans le monde virtuel, c'est par exemple un accès à un forum privé avec l'accord du gestionnaire ('la porte est ouverte'). L'intrusion dans la vie privée est limitée.

Cette méthode n'étant pas plus intrusive que les autres méthodes ordinaires (recours à une source, observation dans des lieux accessibles au public, …), il a été décidé d'en faire également une méthode ordinaire. Cela entre donc dans le même cadre et le même esprit que les autres méthodes ordinaires. En effet, le principe est une discussion libre avec des personnes qui choisissent de dire ce qu'elles veulent.

"*het feit dat een agent, buiten de gevallen bedoeld in artikel 18, zich doelbewust in een groep of in het leven van een persoon integreert om informatie of gegevens te verzamelen, in het kader van een onderzoek door een inlichtingen- en veiligheidsdienst en in het belang van de uitoefening van zijn opdrachten, hetzij in de virtuele wereld, hetzij in de reële wereld. Deze agent verbergt zijn hoedanigheid van agent van de inlichtingen- en veiligheidsdiensten, en voor de agenten van de Algemene Dienst Inlichtingen en Veiligheid, van lid van het ministerie van Defensie, en:*

a) hij neemt deel aan activiteiten of maakt ze mogelijk, of hij ondersteunt actief de overtuigingen of de activiteiten van de persoon of de groep die het voorwerp uitmaakt van het onderzoek, of

b) hij onderhoudt duurzame relaties met hen".

Artikel 16/5 heeft geen betrekking op die gevallen waarbij het internet wordt gebruikt door agenten en bronnen als onderling communicatiemiddel (via e-mail bijvoorbeeld). Het gaat daar niet om een infiltratie, maar om de reguliere contactname tussen beide partners. Op die contacten blijft het artikel 18 van toepassing.

Er wordt ook gepreciseerd dat voor de observatie op het internet in open bronnen (art. 13) met gebruik van een reeds toegestane ondersteuningsmaatregel (art. 13/2) geen nieuwe regelgeving vereist is.

Wanneer de voorwaarden voorzien in de definitie van infiltratie niet vervuld zijn, is het verzamelen van informatie in de virtuele wereld in het algemeen gebaseerd op de bevoegdheid tot het algemeen verzamelen van informatie door middel van open bronnen en contactpersonen, en naar analogie van observaties in de echte wereld.

Aangezien deze methode het 'virtuele equivalent' is van de artikelen 16/1 en 17 W.I.&V, die twee gewone methoden zijn, hebben de opstellers er logischerwijs voor gekozen om hier ook een gewone methode van te maken. Wat wordt beoogd met de infiltratie in de virtuele wereld, is bij voorbeeld de toegang tot een privéforum met instemming van de beheerder ('de deur staat open'). De aantasting van het privéleven is beperkt.

Aangezien die methode niet ingrijpender is dan de andere gewone methoden (inzet van een bron, observatie in voor het publiek toegankelijke plaatsen …), werd er beslist om er ook een gewone methode van te maken. Dit past dus binnen hetzelfde kader en dezelfde geest als de andere gewone methoden. Het principe is immers een vrije discussie met personen die zelf kiezen wat ze willen zeggen.

Néanmoins, lorsque l'agent utilise une identité ou une qualité fictive, au sens des nouvelles définitions prévues à l'article 3, 24° ou 25° de la LRS, pour s'infiltrer dans le monde virtuel, les auteurs du projet ont estimé qu'un encadrement renforcé était nécessaire. Dans ce cas, c'est la nouvelle méthode spécifique de recueil de données d'infiltration virtuelle (article 18/5/1) qui s'appliquera.

Enfin, si le service de renseignement concerné devait "forcer une porte", "craquer un mot de passe", il est évident qu'on tomberait dans le champ d'application de la méthode exceptionnelle d'intrusion informatique visée à l'article 18/16 ou 44/1 de la LRS.

L'infiltration dans le monde virtuel, tout comme la commission d'infraction, répondent ainsi à un besoin réel pour les deux services de renseignement, et ce pour lutter contre toutes les menaces: ainsi certains forums peuvent contenir des informations extrêmement utiles dans la lutte contre l'ingérence, et pour y être accepté, il faut fréquemment montrer qu'on partage certaines convictions et dès lors souvent commettre des infractions (par exemple partager de la propagande nazie ou salafo-djihadiste) …

A titre d'exemple, cette méthode vise l'hypothèse où un agent d'un service de renseignement crée une légende et un pseudonyme et interagit avec la personne objet de son enquête avec cette légende et ce pseudonyme sur les réseaux sociaux et les plateformes de messagerie cryptée en soutenant activement ses convictions et en développant des relations durables avec elle.

Art. 17

Dans la sous-section relative aux méthodes ordinaires de recueil des données de la LRS, un article 16/6 est inséré.

L'idée qui sous-tend l'insertion de cette nouvelle disposition s'inspire de l'article 18/15 actuel de la LRS. Cette dernière disposition offre aux services de renseignement et de sécurité la possibilité de requérir certaines données auprès de banques et d'institutions financières:

— la liste des comptes bancaires, des coffres bancaires ou des instruments financiers définis à l'article 2, 1°, de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers dont la personne

Wanneer de agent in zijn interactie met de geviseerde personen echter een fictieve identiteit of hoedanigheid gebruikt, in de zin van de nieuwe definities voorzien in artikel 3, 24° of 25° van de WIV, om te infiltreren in de virtuele wereld, is er volgens de opstellers van het wetsontwerp een strengere regeling nodig. In dat geval zal de nieuwe specifieke methode voor het verzamelen van gegevens, de virtuele infiltratie (artikel 18/5/1), van toepassing zijn.

Daarentegen, als de betrokken inlichtingendienst "een deur forceert" of "een wachtwoord kraakt", is het duidelijk dat we onder het toepassingsgebied van een uitzonderlijke methode vallen, nl. het binnendringen van een informaticasysteem overeenkomstig artikel 18/16 of 44/1 van de WIV.

De infiltratie in de virtuele wereld beantwoordt op die manier, net als de mogelijkheid om misdrijven te plegen, aan een reële behoefte voor de twee inlichtingendiensten, en dit om alle dreigingen te bekampen: sommige fora kunnen uiterst nuttige informatie bevatten in de strijd tegen inmenging en om daar te worden aanvaard, moet men regelmatig tonen dat men bepaalde overtuigingen deelt en dus vaak inbreuken plegen (bijvoorbeeld het delen van nazi- of salafistisch-jihadistische propaganda).

Bij wijze van voorbeeld: deze methode beoogt de hypothese dat een agent van een inlichtingendienst een legende en een pseudoniem creëert, en aan de hand van die legende en pseudoniem op sociale netwerken en versleutelde berichtenplatformen contact heeft met de persoon die het voorwerp is van zijn onderzoek. De agent ondersteunt daarbij actief de overtuigingen van die persoon en bouwt duurzame relaties met hem op.

Art. 17

Een artikel 16/6 wordt in de onderafdeling betreffende de gewone methoden voor het verzamelen van gegevens van de WIV gevoegd.

De achterliggende gedachte tot invoeging van deze nieuwe bepaling vertrekt vanuit het huidige artikel 18/15 WIV. Laatstgenoemde bepaling geeft de inlichtingen- en veiligheidsdiensten de mogelijkheid om bij banken en financiële instellingen bepaalde gegevens te vorderen:

— de lijst van bankrekeningen, bankkluizen of financiële instrumenten zoals bedoeld in artikel 2, 1° van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, waarvan

visée est titulaire, mandataire ou le bénéficiaire effectif, et, le cas échéant, toutes les données à ce sujet;

— les transactions bancaires qui ont été réalisées, pendant une période déterminée, sur un ou plusieurs de ces comptes bancaires ou instruments financiers, y compris les informations concernant tout compte émetteur ou récepteur;

— les données concernant les titulaires ou mandataires qui, pendant une période déterminée, ont ou avaient accès à ces coffres bancaires.

La collecte de données concernant des comptes bancaires, des coffres bancaires et certains instruments financiers et transactions bancaires est une mesure essentiellement axée sur la surveillance de transactions et de flux financiers suspects.

La compétence d'enquête visée à l'article 18/15 de la LRS concerne une méthode exceptionnelle. La mise en œuvre de cette catégorie de méthodes est soumise à de nombreuses conditions. Ainsi, il ne peut y être fait usage qu'en cas de menace potentielle grave. En outre, la mise en œuvre de telles méthodes s'effectue uniquement dans le respect des principes de subsidiarité et de proportionnalité définis par la loi du 30 novembre 1998. Les agents de renseignement ne peuvent décider de manière autonome de recourir à une méthode exceptionnelle. Cette décision revient exclusivement au dirigeant du service de renseignement et de sécurité concerné, à savoir l'administrateur général de la Sûreté de l'État et le chef du Service Général du Renseignement et de la Sécurité. La décision du dirigeant du service est toujours motivée par écrit de façon circonstanciée. En outre, la méthode ne peut être mise en œuvre qu'après avis conforme de la Commission BIM, une commission indépendante du pouvoir exécutif composée de trois magistrats (un juge d'instruction, également président de la commission, un juge et un magistrat du parquet). De même, la mise en œuvre des méthodes exceptionnelles fait l'objet d'un contrôle interne ainsi que d'un double contrôle externe. Le contrôle interne est mené par le dirigeant du service, qui doit être régulièrement informé du déroulement de la méthode par l'officier de renseignement désigné à cet effet; la Commission BIM et le Comité permanent R sont chargés du contrôle externe. Enfin, les méthodes exceptionnelles ne peuvent être utilisées que dans le cadre du travail de renseignement, et non dans celui des enquêtes ou des vérifications de sécurité.

Le seuil minimal permettant aux services de renseignement et de sécurité d'ouvrir une enquête financière est trop élevé à l'heure actuelle. Dans le cadre d'une

de geviseerde persoon titularis, gevolmachtigde of de uiteindelijk gerechtigde is, en, in voorkomend geval alle nadere gegevens hieromtrent;

— de bankverrichtingen die in een bepaald tijdvak zijn uitgevoerd op één of meerdere van deze bankrekeningen of financiële instrumenten, met inbegrip van de bijzonderheden betreffende de rekening van herkomst of bestemming;

— de gegevens met betrekking tot de titularissen of gevolmachtigden, die in een bepaald tijdvak toegang hebben of hadden tot deze bankkluizen.

Het inwinnen van gegevens over bankrekeningen, bankkluizen, bepaalde financiële instrumenten en banktransacties is een maatregel die vooral gericht is op het toezicht op bepaalde verdachte geldstromen en -transacties.

De in artikel 18/15 WIV bepaalde onderzoeksbevoegdheid betreft een uitzonderlijke methode. De uitvoering van deze categorie van methoden is onderworpen aan heel wat voorwaarden. Zo mag er slechts gebruik van gemaakt worden wanneer er sprake is van een ernstige potentiële dreiging. Daarnaast is de aanwending slechts mogelijk indien aan de in de wet van 30 november 1998 bepaalde subsidiariteits- en proportionaliteitseis wordt voldaan. De inlichtingenagenten mogen niet autonoom beslissen om een uitzonderlijke methode aan te wenden. Die beslissing komt alleen toe aan het diensthoofd van de betrokken inlichtingen- en veiligheidsdienst, zijnde de administrateur-generaal van de Veiligheid van de Staat en de chef van de Algemene Dienst Inlichting en Veiligheid. De beslissing van het diensthoofd is steeds schriftelijk en omstandig gemotiveerd. Daarenboven mag de methode pas worden uitgevoerd na het verkrijgen van een eensluidend advies van de BIM-Commissie, een onafhankelijk van de uitvoerende macht bestaande commissie bestaande uit drie magistraten (een onderzoeksrechter, tevens commissievoorzitter, een rechter en een parketmagistraat). Ook is de uitvoering van de uitzonderlijke methoden onderworpen aan een interne en een dubbele externe controle. De interne controle gebeurt door het diensthoofd die door de hiertoe aangestelde inlichtingenofficier regelmatig moet geïnformeerd worden over het verloop van de methode; de externe controle wordt uitgevoerd door de BIM-Commissie en door het Vast Comité I. Ten slotte mogen de uitzonderlijke methoden alleen gehanteerd worden in het kader van het inlichtingenwerk, niet in het kader van veiligheidsonderzoeken of -verificaties.

De minimumdrempel voor de inlichtingen- en veiligheidsdiensten om een financieel onderzoek te starten is momenteel te hoog. In het kader van een

enquête de renseignement, on ne peut pas toujours établir clairement quels sont les comptes bancaires, les coffres bancaires ou (comme mentionné plus haut) les instruments financiers dont une personne visée dispose et, le cas échéant, auprès de quelle banque. L'obtention d'une réponse à cette question est actuellement soumise au régime strict des méthodes exceptionnelles.

Si le caractère intrusif d'une telle méthode est considéré comme faible à très faible étant donné que l'accent n'est pas mis sur l'obtention d'un aperçu de la situation financière d'un individu ou d'un groupement (par ex. au moyen du montant qui se trouve sur le compte bancaire), ni sur la vérification des personnes avec lesquelles la personne visée entretient des contacts sur le plan financier (par ex. par le biais des transactions effectuées sur un compte bancaire ou via un coffre-bancaire dans un délai donné), ni sur les mouvements enregistrés sur ces comptes par le passé ou dans le futur, l'acte d'enquête susvisé (intervenant souvent en premier lieu) est néanmoins soumis aux mêmes exigences strictes que toutes les autres méthodes exceptionnelles qui peuvent cependant impliquer une atteinte à la vie privée bien plus importante.

L'exigence relative à la présence d'une menace potentielle "grave" et à la motivation renforcée qui en découle, sont pleinement justifiées en ce qui concerne la demande d'informations sur des transactions de nature financière, et non à des fins de simple identification de comptes bancaires, de coffres bancaires ou de certains instruments financiers dont la personne visée est le titulaire, le mandataire ou le véritable bénéficiaire, ni d'identification du titulaire, du mandataire ou véritable bénéficiaire de certains instruments financiers.

Le gouvernement estime souhaitable que cette compétence, à l'instar de la compétence similaire pour les demandes de données d'identification auprès des opérateurs de services de communications électroniques et des fournisseurs de services de communications électroniques (*cf.* article 16/2 de la LRS) soit qualifiée de méthode ordinaire.

Pour répondre au point 70 de l'avis du Comité R et à l'avis de la Commission BIM (p.6), les auteurs du projet réaffirment que le lien qui est fait entre la personne visée par l'identification des produits et services financiers se limite aux données d'identification et ne donnent dès lors pas d'informations sur la capacité financière de la personne. L'intrusion dans la vie privée étant comparable à la méthode ordinaire d'identification de données auprès des opérateurs et des fournisseurs de services de communications électroniques (art. 16/2), les auteurs

inlichtingenonderzoek is het niet steeds duidelijk over welke bankrekeningen, bankkluizen of (zoals hiervoor bepaalde) financiële instrumenten een geviseerd persoon beschikt, en zo ja, bij welke bank. Het verkrijgen van een antwoord op deze vraag is momenteel echter onderworpen aan het strenge regime van de uitzonderlijke methoden.

Hoewel de intrusieve aard van een dergelijke methode gering tot zeer gering is, gezien het niet gericht is op het verkrijgen van een zicht op de financiële situatie van een individu of groepering (bv. via het bedrag dat op een bankrekening staat), noch op het nagaan met welke personen de geviseerde persoon financieel in contact staat (bv. via de binnen een bepaalde tijdspanne gedane verrichtingen op een bankrekening of -kluis), noch op welke bewegingen die rekeningen in het verleden maakten of in de toekomst maken, is vernoemde (veelal eerste) onderzoeksdaad niettemin aan dezelfde stringente eisen onderworpen als alle andere uitzonderlijke methoden, die nochtans een veel verregaande inbreuk op het privéleven kunnen inhouden.

De vereiste van de aanwezigheid van een 'ernstige' potentiële dreiging, en de hieruit voortvloeiende verstrengde en verzwaarde motiveringseis, die zeker wel verantwoord is voor wat betreft het opvragen van 'informatie inzake verrichtingen van financiële aard', is dit echter niet voor het louter identificeren van bankrekeningen, bankkluizen of bepaalde financiële instrumenten waarvan de geviseerde persoon titularis, gevolmachtigde of de uiteindelijke gerechtigde is, noch voor het identificeren van de titularissen, de gevolmachtigden, of de uiteindelijke gerechtigden van bankrekeningen, bankkluizen of bepaalde financiële instrumenten.

De regering acht het wenselijk deze bevoegdheid, net zoals de vergelijkbare bevoegdheid tot het opvragen van identificatiegegevens bij de operatoren van elektronische communicatiediensten en de verstrekkers van elektronische communicatiediensten (*cf.* artikel 16/2 WIV), te kwalificeren als een gewone methode.

Om te antwoorden op punt 70 van het advies van het Comité I, en het advies van de BIM-Commissie (p.6), bevestigen de auteurs van het ontwerp dat het verband dat wordt gelegd tussen de geviseerde persoon, door de identificatie van financiële producten en diensten, beperkt blijft tot identificatiegegevens. Deze geven geen informatie over het financieel vermogen van de persoon. De intrusie in het privéleven is vergelijkbaar met de gewone methode van identificatie van gegevens bij de operatoren en de verstrekkers van een elektronische

estiment avoir suffisamment justifié le fait d'en faire une méthode ordinaire.

En ce qui concerne la collecte de données auprès de banques et d'institutions de crédit, il y a lieu, dans le contexte du travail de renseignement, et comme dans celui de la collecte d'informations dans le secteur des télécommunications, d'établir une distinction entre la compétence de prise de connaissance de simples données d'identification et la compétence de prise de connaissance du contenu des données. En outre, une réponse positive à la question de savoir si une personne visée possède un compte dans une banque spécifique sera suivie en principe d'une application de l'article 18/15 de la LRS (qui est et restera une méthode exceptionnelle). Grâce à cette adaptation, une réponse négative, qui représente déjà en soi une information essentielle dans une enquête de renseignement, relèvera plus rapidement des possibilités d'enquête.

Quant au champ d'application ratione personae de l'article 16/6 de la LRS, il est tenu compte de l'extension du champ d'application de l'article 46*quater* du Code d'instruction criminelle et de l'article 18/15 de la LRS. De même, le Point de Contact Central (PCC) tenu par la Banque nationale de Belgique est ajouté à la liste des personnes et des instances pouvant être requises (voir commentaires aux dispositions modifiant les articles de loi en question). La coopération du PCC s'effectue également en prenant compte des dispositions spécifiques inscrites à la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt. Une adaptation a été introduite pour rendre possible la procédure d'extrême urgence.

Si, dans le cas d'extrême urgence, la réquisition écrite n'est pas envoyée dans le délai de 24 heures, l'institution peut contacter le service concerné. Si le service n'y donne pas suite, l'institution peut le mentionner au Comité permanent R.

Il est par ailleurs à noter qu'à l'instar des articles 16/2, 16/3 et 16/4 de la LRS, deux garanties supplémentaires ont été intégrées dans l'article 16/6 de la LRS, qui ne s'appliquent pas aux autres méthodes ordinaires de renseignement.

Tout d'abord, cette compétence ne peut être exercée par n'importe quel acteur des services de renseignement et de sécurité: la réquisition doit être effectuée par l'intermédiaire du dirigeant du service ou de son délégué. Il s'agit là d'une transposition au sein des services de

communicatiedienst (art. 16/2). Daarom zijn de auteurs van mening voldoende te hebben gemotiveerd dat dit een gewone methode wordt.

Met betrekking tot het inwinnen van gegevens bij banken en kredietinstellingen dient binnen het inlichtingenwerk, net zoals bij de informatiegaring bij de telecomsector, een onderscheid gemaakt te worden tussen de bevoegdheid tot kennisname van louter identificatiegegevens en de bevoegdheid tot kennisname van de inhoud. Een positief antwoord op de vraag of een geviseerd persoon een bankrekening bij een bepaalde bank heeft, zal daarenboven in principe gevolgd worden door een toepassing van artikel 18/15 WIV (die een uitzonderlijke methode is en blijft). Een negatief antwoord, die op zich reeds een belangrijke informatie is binnen een inlichtingenonderzoek, zal door deze aanpassing voortaan sneller tot de onderzoeksmogelijkheden behoren.

Voor wat betreft het toepassingsgebied ratione personae van artikel 16/6 WIV, wordt rekening gehouden met de uitbreiding van het toepassingsgebied van artikel 46*quater* Sv en artikel 18/15 WIV. Ook het Centraal Aanspreekpunt (CAP) gehouden door de Nationale Bank van België wordt toegevoegd aan de lijst van personen en instanties die gevorderd kunnen worden (zie commentaar bij de bepalingen die betrokken wetsartikelen wijzigen). De medewerking van het CAP gebeurt eveneens rekening houdend met de specifieke bepalingen die zijn ingeschreven in de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van bankrekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest. Een aanpassing werd doorgevoerd om een procedure van hoogdringendheid in te voeren.

In het geval de schriftelijke vordering bij hoogdringendheid niet binnen de termijn van 24 uur overgemaakt wordt, kan de instelling de betreffende dienst contacteren. Indien de dienst hieraan geen gevolg geeft, kan de instelling dit melden bij het vast Comité I.

Van belang is dat daarnaast, net zoals in de artikelen 16/2, 16/3 en 16/4 WIV, twee bijkomende garanties werden ingebouwd in artikel 16/6 WIV, die niet gelden voor de andere gewone inlichtingenmethoden.

Vooreerst kan niet eender welke actor binnen de inlichtingen- en veiligheidsdiensten de bevoegdheid uitoefenen: de vordering moet gebeuren door het diensthoofd of zijn gedelegeerde. Dit is een vertaling naar de inlichtingen- en veiligheidsdiensten van de regeling die

renseignement et de sécurité du règlement en vigueur pour les services de police, lesquels n'étant habilités à requérir de telles données qu'après accord du procureur du Roi (*cf.* article 46*quater* du Code d'instruction criminelle). D'un point de vue opérationnel, le dirigeant d'un service de renseignement et de sécurité se trouve au même niveau que le procureur du Roi étant donné que tous deux assurent la direction de l'enquête.

A titre de deuxième garantie complémentaire, les services de renseignement et de sécurité doivent tenir un registre des identifications requises afin de permettre au Comité permanent R d'exercer un contrôle sur ces méthodes de renseignement. Si, sur la base de l'analyse de ces données, le Comité permanent R devait constater des problèmes en termes de légalité ou d'efficacité, il peut ouvrir une enquête de contrôle et informer le Parlement ainsi que les ministres compétents des résultats de l'enquête. Dans ses rapports à la Commission d'accompagnement du Comité permanent R et du Comité permanent P au sein de la Chambre des représentants, le Comité permanent R devra aussi accorder une attention particulière à la façon dont les deux services de renseignement et de sécurité utiliseront cette compétence.

De plus, à l'instar de l'obligation de collaboration prévue à l'article 18/15 de la LRS et des autres obligations de collaboration visées dans la loi du 30 novembre 1998 (secteur des télécommunications, de la poste, des voyages et des transports), une obligation de collaboration spécifique est introduite dans l'article 16/6.

La sanction pénale liée à l'obligation de collaboration est la même que celle prévue à l'article 18/15 de la LRS, modifiée de manière générale et uniforme par la loi du 30 mars 2017.

La dernière modification effectuée après les avis (dans la version française uniquement, les mots "dans les conditions" sont remplacés par "dans des conditions" et "les conditions légales" par "les dispositions légales"") est une simple correction technique suite à une erreur de formulation et ne modifie pas la portée de cet article.

Art. 18

1. But des présentes modifications aux articles 18, 18/1, 18/3, 18/9, 18/10 LRS

L'article 18 de la LRS dispose que les services de renseignement peuvent avoir recours aux sources humaines pour la collecte d'informations dans l'intérêt de l'exercice de leurs missions.

geldt voor de politiediensten. Deze laatsten kunnen de betreffende gegevens slechts opvragen na akkoord van de procureur des Konings (*cf.* artikel 46*quater* Sv.). Het diensthoofd van een inlichtingen- en veiligheidsdienst bevindt zich operationeel gezien op dezelfde hoogte als de procureur des Konings, gezien beiden de leiding hebben over het onderzoek.

Als tweede bijkomende garantie moeten de inlichtingen- en veiligheidsdiensten een register bijhouden van de gevorderde identificaties om aldus het Vast Comité I toe te laten toezicht uit te oefenen over deze inlichtingenmethoden. Mocht het Vast Comité I op basis van de analyse van deze gegevens vaststellen dat er zich problemen aandienen op het vlak van rechtmatigheid of efficiëntie, kan het steeds een toezichtonderzoek openen en het Parlement en de bevoegde ministers inlichten van de resultaten. Daarenboven zal het Vast Comité I in zijn verslagen aan de Begeleidingscommissie van het Vast Comité I en het Vast Comité P bij de Kamer van volksvertegenwoordigers specifiek aandacht moeten besteden aan de wijze waarop de twee inlichtingen- en veiligheidsdiensten deze bevoegdheid hanteren.

Net zoals de medewerkingsplicht in artikel 18/15 WIV en de overige medewerkingsplichten in de wet van 30 november 1998 (telecom-, post-, reis- en vervoersector) wordt er in artikel 16/6 WIV een bijzondere medewerkingsplicht ingesteld.

De aan de medewerkingsplicht gekoppelde strafsanctie is dezelfde als die van artikel 18/15 WIV, zoals deze door de wet van 30 maart 2017 op algemene en uniforme manier werd gewijzigd.

De laatste wijziging na de adviezen (het vervangen, enkel in de Franse tekst, van de woorden "dans les conditions" door "dans des conditions" en van de woorden "de wettelijke voorwaarden" door "de wettelijke bepalingen") is een louter technische verbetering van een foutieve verwoording en wijzigt de draagwijdte van dit artikel niet.

Art. 18

1. Doel van de voorgestelde wijzigingen van artikelen 18, 18/1, 18/3, 18/9, 18/10 WIV

Artikel 18 van de WIV bepaalt dat de inlichtingendiensten beroep kunnen doen op menselijke bronnen voor het verzamelen van informatie die van belang is voor de uitoefening van hun opdrachten.

Etant donné qu'une définition de "source humaine" a maintenant été introduite dans la LRS (voir l'article 3, 26°), et que celle-ci précise qu'il s'agit de personnes enregistrées dans le registre des sources, l'article 18 doit être légèrement adapté afin que les services de renseignement gardent une base légale pour discuter avec des contacts qui ne sont pas (encore) inscrits dans le registre des sources. Les mots "à des personnes dont" les sources humaines ont donc été ajoutés.

Il va de soi que les sources humaines au sens du nouveau 26° de l'article 3 avec lesquelles les services coopèrent doivent être fiables, loyales et discrètes. De plus, la source ne doit pas être exposée à une pression externe ou manipulée par d'autres personnes. Travailler avec une source qui fournit des informations incorrectes peut entraîner la prise de mauvaises décisions ou l'échec des opérations. Une source qui est mise sous pression ou manipulée peut également courir un risque pour sa personne.

Les présentes modifications visent à introduire la possibilité d'effectuer des méthodes de recueil de données spécifiques ou exceptionnelles (ci-après BIM) sur une source humaine lorsque celle-ci est inscrite dans le registre des sources humaines des services de renseignement et de sécurité et qu'il existe un doute quant à sa fiabilité, sa discrétion ou sa loyauté. Le registre contient les noms des personnes qui sont déjà sources ou en cours de recrutement par les services de renseignement et de sécurité et qui ont fait l'objet d'une validation hiérarchique. Cette limitation aux personnes inscrites dans le registre restreint le champ d'application de la présente disposition.

Il est également prévu de pouvoir exécuter une BIM sur une source humaine afin d'assurer sa propre sécurité.

Cette nouvelle compétence de pouvoir effectuer une BIM sur une source est essentielle afin de contrôler, notamment, la fiabilité, la discrétion ou la loyauté de la source vis-à-vis des services de renseignement et de sécurité. Ceci permet de mieux sécuriser la relation qui est développée entre l'agent désigné pour encadrer la source et cette dernière. Cette possibilité permettra aussi de renforcer la protection de l'intégrité physique, psychique et morale de la source.

Le nouveau paragraphe 2 précise que c'est bien dans l'intérêt de l'exercice de leurs missions visées aux articles 7, 1° et 3°/1 et 11, § 1, 1° à 3° et 5° de la LRS que les services de renseignement peuvent mettre en œuvre l'ensemble des méthodes de recueil de données,

Aangezien er nu in de WIV een definitie van "menselijke bron" werd ingevoegd (zie artikel 3, 26°), en daar deze verduidelijkt dat het gaat om personen die geregistreerd zijn in het register van bronnen, dient het artikel 18 licht te worden aangepast, zodat de inlichtingendiensten een wettelijke basis behouden om te overleggen met contactpersonen die (nog) niet in het register van bronnen zijn ingeschreven. De woorden "op personen waaronder" menselijke bronnen werden daarom ingevoegd.

Het spreekt voor zich dat de menselijke bronnen in de zin van het nieuwe 26° van artikel 3, waarmee de dienst samenwerkt betrouwbaar moeten zijn en zich loyaal en discreet opstellen. Ook mag de bron niet aan druk van buiten uit blootgesteld worden of door anderen gemanipuleerd worden. Werken met een bron die onjuiste informatie verstrekt, kan ertoe leiden dat de dienst verkeerde beslissingen neemt of dat operaties mislukken. Een bron die onder druk gezet of gemanipuleerd wordt, kan daarenboven ook persoonlijk gevaar lopen.

Het doel van deze wijzigingen is het introduceren van de mogelijkheid om specifieke of uitzonderlijke methoden voor het verzamelen van gegevens (hierna BIM) op een menselijke bron die is ingeschreven in het register van de menselijke bronnen van de inlichtingen- en veiligheidsdiensten toe te passen wanneer er twijfel bestaat over diens betrouwbaarheid, discretie of loyaliteit. Dit register bevat de namen van personen die al bronnen zijn of worden gerekruteerd door de inlichtingen- en veiligheidsdiensten en die het voorwerp hebben uitgemaakt van een hiërarchische validatie. De beperking tot deze personen ingeschreven in het register, beperkt de reikwijdte van deze bepaling.

Er wordt ook in de mogelijkheid voorzien om een BIM op een menselijke bron uit te voeren om zijn eigen veiligheid te garanderen.

Deze nieuwe bevoegdheid om een BIM op een bron uit te voeren, is essentieel teneinde, in het bijzonder, de betrouwbaarheid, de discretie of de loyaliteit van de bron ten opzichte van de inlichtingen- en veiligheidsdiensten te controleren. Dit maakt het mogelijk om de relatie die wordt ontwikkeld tussen de agent aangeduid om de bron te begeleiden en deze laatste te verzekeren. Deze mogelijkheid versterkt tevens de mogelijkheid om de fysieke, psychische en morele integriteit van de bron te vrijwaren.

De nieuwe paragraaf 2 preciseert dat de inlichtingendiensten alle methoden voor het verzamelen van gegevens kunnen implementeren in het belang van de uitvoering van hun opdrachten als bedoeld in de artikelen 7, 1° en 3°/1 en 11, § 1, 1° tot 3° en 5° van de WIV,

c'est-à-dire, les méthodes ordinaires, spécifiques et/ou exceptionnelles.

Il est également précisé qu'il faut:

— Soit un doute quant à la fiabilité, la discrétion ou la loyauté de la source humaine qui est inscrite dans le registre des sources humaines susceptible de causer un préjudice pour l'exercice des missions du service de renseignement avec lequel la source collabore (art. 18§ 2, 2°). Cette précision est importante car il n'est bien évidemment pas question d'effectuer des méthodes de recueil de données spécifiques et exceptionnelles systématiquement sur toutes les sources d'un service de renseignement. Ceci sera donc pris en compte lors de l'évaluation du principe de proportionnalité et de subsidiarité;

— Soit pour assurer la protection de la source humaine.

Pour répondre au point 73 de l'avis du Comité R, il n'est pas ajouté "ou qui complique le suivi de cette menace" car les auteurs du projet ont préféré parler de "préjudice pour l'exercice des missions" du service de renseignement plutôt que de "menace". Cela évite la confusion avec les menaces visées aux articles 8 et 11 de la LRS. En effet, il n'est pas question ici des mêmes menaces. Par exemple, l'intégrité physique d'un agent d'un service de renseignement pourrait être menacée parce qu'une source le dénonce. Il n'est donc pas question de menace au sens des missions des services de renseignement (terrorisme, extrémisme, espionnage, ingérence, …), mais d'atteinte au bon accomplissement des missions du service de renseignement ou à la sécurité de son personnel qui pourraient être préjudiciés, par exemple, par des informations erronées.

2. Explication détaillée des modifications proposées

a) Le principe de proportionnalité

A l'heure actuelle, effectuer une BIM sur une personne, conformément aux dispositions légales, nécessite qu'on puisse toujours justifier de la menace potentielle qu'elle représente. Pour exécuter une méthode de recueil de données spécifique, il faut justifier d'une menace potentielle, et pour exécuter une méthode exceptionnelle, il faut justifier d'une menace potentielle grave. La menace dont il est question est celle visée aux articles 7, 1° et 3°/1 et 11, § 1, 1° à 3° et 5° de la LRS. La Commission administrative chargée du contrôle des méthodes spécifiques et exceptionnelles (ci-après "Commission BIM") doit évaluer la proportionnalité de la méthode en fonction de cette menace potentielle. Ce principe de proportionnalité

dat wil zeggen gewone, specifieke en/of uitzonderlijke methoden.

Er wordt ook verduidelijkt dat er:

— ofwel twijfel moet bestaan over de betrouwbaarheid, discretie of loyauteit van de menselijke bron die is opgenomen in het register van menselijke bronnen, waardoor er een nadeel ontstaat voor de uitoefening van de opdrachten van de inlichtingendienst waarmee de bron samenwerkt (art. 18§ 2, 2°). Deze precisering is belangrijker gezien er uiteraard geen sprake is van het systematisch toepassen van specifieke en uitzonderlijke methoden voor het verzamelen van gegevens op alle bronnen van een inlichtingendienst. Dit zal daarom in aanmerking worden genomen bij de beoordeling van het evenredigheidsbeginsel en het subsidiariteitsbeginsel;

— Ofwel voor het verzekeren van de bescherming van de menselijke bron.

Om te antwoorden op punt 73 van het advies van het Comité I werd "of die de opvolging van deze dreiging bemoeilijkt" niet toegevoegd, omdat de auteurs van het ontwerp liever spreken over "een nadeel voor de uitoefening van de opdrachten" van de inlichtingendienst, dan over "een bedreiging". Dit vermijdt verwarring met de bedreigingen bedoeld in artikelen 8 en 11 van de WIV. Het gaat hier immers niet om dezelfde bedreigingen. Bij voorbeeld, de fysieke integriteit van een agent van een inlichtingendienst kan worden bedreigd omdat een bron hem verklikt. Er is dan geen sprake van een bedreiging in de zin van de opdrachten van de inlichtingendiensten (terrorisme, extremisme, spionage, inmenging, …), maar van een gevaar voor de goede uitoefening van de opdrachten van de inlichtingendienst, of voor de veiligheid van haar personeel, die benadeeld kunnen worden door, bij voorbeeld, foutieve informatie.

2. Toelichting in detail van de voorgestelde wijzigingen

a) Het evenredigheidsbeginsel

Op dit moment vereist het uitvoeren van een BIM op een persoon, in overeenstemming met de wettelijke bepalingen, dat de potentiële bedreiging die vanuit een persoon uitgaat, wordt aangetoond. Om een specifieke methode uit te voeren, is het noodzakelijk om een potentiële bedreiging te rechtvaardigen en om een uitzonderlijke methode uit te voeren, moet men een ernstige potentiële bedreiging rechtvaardigen. De bedreiging waarvan sprake is deze waarnaar wordt verwezen in de artikelen 7, 1° en 3°/1 en 11, § 1, 1° tot 3° en 5° van de WIV. De administratieve commissie die belast is met de controle van specifieke en uitzonderlijke methoden (hierna "BIM-Commissie" genoemd) moet de proportionaliteit

prévoit qu'on doit choisir une méthode spécifique ou exceptionnelle en fonction du degré de gravité de la menace potentielle pour laquelle elle est mise en œuvre.

Or, pour une source humaine avec laquelle les services de renseignement et de sécurité envisagent de collaborer ou collaborent déjà, les menaces prévues par la LRS ne sont pas toujours justifiables. Par contre, les risques de manque de fiabilité sont toujours présents. Il existe donc une autre menace qui est différente de celle prévue actuellement. En effet, lorsqu'une source est en cours de recrutement ou qu'elle est déjà traitée, il existe toujours un risque que la personne approchée ou recrutée se retourne contre le service de renseignement et de sécurité. Il est dès lors essentiel que les services de sécurité et de renseignement puissent contrôler la fiabilité, la discrétion et la loyauté pour renforcer leur choix et leur profilage.

Par conséquent, le principe de proportionnalité prévu à l'article 2, § 1er, alinéa 4, à l'article 18/3 § 2 et à l'article 18/9, § 2 doit être évalué différemment lorsque les services de renseignement et de sécurité appliquent le nouveau paragraphe 2 de l'article 18. Le principe de proportionnalité est un principe général de droit, qui inspire toute autorité administrative lorsqu'elle porte atteinte à un droit fondamental, tel que l'atteinte à la vie privée. L'essence de ce principe est de vérifier la juste mesure entre la décision qui fait grief, tel que le fait d'effectuer une BIM sur une source, et les faits qui l'ont entraîné ou le but poursuivi. L'autorité publique doit prendre une mesure qui doit être à la fois respectueuse des intérêts de la personne visée par la BIM et des objectifs d'intérêt général poursuivis par son administration.

Dans le cadre du nouveau paragraphe 2 de l'article 18, l'évaluation du principe de proportionnalité portera sur le préjudice:

— que le service concerné est susceptible d'encourir s'il y a un doute sur la fiabilité, la discrétion et/ou la loyauté de la source;

ou

— à l'encontre de la source elle-même qui justifie le besoin d'assurer sa protection.

Par conséquent, lors de l'application du nouveau paragraphe 2 de l'article 18, ce ne sera plus la menace potentielle telle que visée aux articles 7, 8 et 11 de la LRS

van de methode in functie van deze potentiële dreiging evalueren. Dit proportionaliteitsbeginsel stipuleert dat een specifieke of uitzonderlijke methode moet worden gekozen op basis van de ernst van de potentiële dreiging waarvoor deze wordt toegepast.

Voor een menselijke bron waarmee de inlichtingen- en veiligheidsdiensten voorzien om samen te werken, of reeds samenwerken, zijn de bedreigingen waarin de WIV voorziet niet steeds te rechtvaardigen. De risico's van onbetrouwbaarheid zijn steeds aanwezig. Er bestaat dus een andere dreiging, die verschilt van diegenen die actueel voorzien zijn. Wanneer een bron wordt benaderd of reeds ingezet wordt, bestaat er altijd een risico dat de benaderde of gerekruteerde persoon zich zal keren tegen de inlichtingen- en veiligheidsdienst. Het is daarom essentieel dat de inlichtingen- en veiligheidsdiensten de betrouwbaarheid, discretie en loyaliteit kunnen controleren om hun keuze van de persoon en hun profilering te verbeteren.

Bijgevolg moet het evenredigheidsbeginsel van artikel 2, § 1, vierde lid, artikel 18/3 § 2 en artikel 18/9, § 2 verschillend worden beoordeeld wanneer de inlichtingen- en veiligheidsdiensten gebruik maken van de nieuwe paragraaf 2 van artikel 18. Het evenredigheidsbeginsel is een algemeen rechtsbeginsel dat elke bestuurlijke overheid in acht dient te nemen wanneer het een fundamenteel recht raakt, zoals schending van de persoonlijke levenssfeer. De essentie van dit principe is om de rechtvaardiging te verifiëren tussen de beslissing die aan het fundamenteel recht raakt, zoals het toepassen van een BIM op een bron, en de feiten die ertoe hebben geleid of het doel dat wordt beoogd. De overheid moet een maatregel nemen die tegelijkertijd rekening houdt met de belangen van de persoon waarop de BIM zich richt, en met doelstellingen van algemeen belang die door haar administratie worden nagestreefd.

In de nieuwe paragraaf 2 van artikel 18 zal de beoordeling van het evenredigheidsbeginsel betrekking hebben op het nadeel:

— dat de betrokken dienst kan ondervinden, indien er twijfel bestaat over de betrouwbaarheid, discretie en / of loyaliteit van de bron;

of

— voor de bron zelf, waardoor de noodzaak tot bescherming ervan wordt gerechtvaardigd.

Daarom zal het bij toepassing van de nieuwe paragraaf 2 van artikel 18, niet langer de potentiële bedreiging zoals bedoeld in de artikelen 7, 8 en 11 van de WIV zijn

qui sera évaluée par la Commission BIM pour accorder la méthode spécifique ou exceptionnelle.

b) Le principe de subsidiarité

Enfin, il est à noter que le principe de subsidiarité reste également d'application: la méthode spécifique est mise en œuvre que si les méthodes ordinaires sont jugées insuffisantes pour permettre de récolter les informations nécessaires à l'évaluation de la fiabilité, la discrétion ou la loyauté de la source humaine. De même, la méthode exceptionnelle ne peut être mise en œuvre que si les méthodes ordinaires ou spécifiques sont jugées insuffisantes pour atteindre ce but.

Enfin, comme prévu à l'article 2, § 1er, lors de l'évaluation du principe de subsidiarité, il est également tenu compte des risques que comporte l'exécution de la mission de renseignement pour la sécurité des agents, des sources humaines et des tiers.

Art. 19

Un nouveau point 3 (3°) est inséré à l'article 18/1 afin d'inclure la référence au nouveau paragraphe 2 de l'article 18 et ainsi étendre le champ d'application matériel pour pouvoir exécuter des BIM sur des sources humaines lorsque les deux conditions cumulatives préalables (inscrite dans le registre des sources humaines et l'existence d'un doute quant à la fiabilité, la discrétion ou la loyauté de la source humaine ou la nécessité d'assurer sa protection) sont remplies.

Il faut rappeler que les BIM sur les sources seront mises en œuvre uniquement lorsque la personne sera déjà inscrite au registre des sources humaines des services de renseignement et qu'il y a un doute sur sa fiabilité, sa discrétion ou sa loyauté ou la nécessité d'assurer sa protection. Le registre contient les noms des personnes qui sont déjà sources ou en cours de recrutement par les services de renseignement et de sécurité et qui ont fait l'objet d'une validation hiérarchique. Il n'est donc pas question d'effectuer une BIM sur n'importe qui. Comme déjà rappelé, la Commission BIM devra en outre toujours évaluer les principes de subsidiarité et de proportionnalité.

Par ailleurs, pour répondre au point 72 de l'avis du Comité R et au point 3 de l'avis du Collège des procureurs généraux, le concept de source humaine est défini à l'article 3, 26° de la LRS: c'est une personne qui donne une information aux services de renseignement et qui est enregistrée suivant la procédure prévue dans la directive

die door de BIM-Commissie zal worden geëvalueerd om de specifieke of uitzonderlijke methode toe te staan.

b) Het subsidiariteitsprincipe

Ten slotte dient te worden opgemerkt dat het subsidiariteitsbeginsel ook van toepassing is: de specifieke methode wordt alleen toegepast indien de gewone methoden als onvoldoende worden geacht om de verzameling van de nodige informatie voor de beoordeling van de betrouwbaarheid, discretie of de loyaliteit van de menselijke bron. Evenzo kan de uitzonderlijke methode alleen worden toegepast als de gewone of specifieke methoden onvoldoende worden geacht voor dit doel te bereiken.

Ten slotte wordt, zoals bepaald in artikel 2, § 1, bij de evaluatie van het subsidiariteitsprincipe eveneens rekening gehouden met de risico's die de uitvoering van de inlichtingenopdracht inhoudt voor de veiligheid van de agenten en van derden.

Art. 19

Een nieuw punt 3 (3°) is in artikel 18/1 opgenomen teneinde de verwijzing naar de nieuwe paragraaf 2 van artikel 18 op te nemen en aldus het materiële toepassingsgebied uit te breiden om een BIM op menselijke bronnen te kunnen uitvoeren wanneer aan beide voorafgaandelijke cumulatieve voorwaarden (opgenomen in het register van menselijke bronnen en het bestaan van twijfel over de betrouwbaarheid, discretie of loyaliteit van de menselijke bron of de noodzaak om de bescherming van de bron te waarborgen) is voldaan.

Er moet aan worden herinnerd dat de BIM op bronnen slechts kan worden uitgevoerd indien de persoon reeds in het register van menselijke bronnen van de inlichtingendiensten is ingeschreven en indien er twijfel over diens betrouwbaarheid, discretie of zijn loyaliteit of de noodzaak tot zijn bescherming bestaat. Het register bevat de namen van personen die reeds bronnen zijn of die zich in het aanwervingsproces van de inlichtingen- en veiligheidsdiensten bevinden en die door de hiërarchie zijn gevalideerd. Een BIM kan niet uitgevoerd worden op ongeacht wie. Zoals reeds in herinnering werd gebracht, zal de BIM-Commissie daarnaast tevens de beginselen van subsidiariteit en evenredigheid moeten nagaan.

Daarenboven, om te antwoorden op punt 72 van het advies van het Comité I en op punt 3 van het advies van het College van procureurs-generaal, wordt het begrip menselijke bron gedefinieerd in artikel 3, 26° van de WIV: het gaat om een persoon die een inlichting meedeelt aan de inlichtingendiensten, en die geregistreerd

classifiée du 25 mars 2019 portant sur le recours à des sources humaines approuvées par le Conseil national de sécurité (voir p. 8 de l'exposé des motifs).

Ainsi, la possibilité de pouvoir faire une BIM sur une source humaine ne pourra être effectuée que sur une source enregistrée au sens de l'article 3, 26° de la LRS et validée par le service de renseignement avec lequel elle collabore. Cette validation implique que la source aura fait l'objet de plusieurs évaluations internes.

Cette précision permet donc d'exclure la possibilité, jugée excessive et trop intrusive dans la vie privée, d'effectuer une BIM sur une personne qu'on envisagerait de recruter comme source afin d'évaluer ses accès et ses contacts.

Art. 20

À l'article 18/2, une précision est ajoutée pour uniformiser les procédures:

comme prévu à l'article 18/10 § 4 (qui décrit la procédure en cas d'extrême urgence pour effectuer une méthode spécifique ou exceptionnelle de recueil de données) et les nouveaux articles 13/1 et 13/1/1 (commission d'infractions par les agents et les sources), lorsque le président de la Commission n'est pas joignable, il peut être remplacé par un autre membre de la Commission.

Pour l'utilisation d'une méthode exceptionnelle à l'égard d'une source humaine, on ne modifie pas le fait qu'une menace potentielle grave devra être justifiée, conformément à l'article 18/9 § 1er, 1° et 2° (respectivement pour la VSSE et le SGRS).

Pour répondre aux avis du Conseil d'État (art. 19) et de la Commission BIM (p. 7), le mot "contacté" est supprimé car en cas d'empêchement du président de la Commission BIM, c'est un "autre membre" qui avertira les présidents des Ordres ou de l'Association des journalistes. En effet, dans le cadre de cette procédure, le membre de la Commission BIM qui remplace le président de la Commission BIM empêché n'est pas formellement "contacté", comme c'est le cas dans la procédure d'extrême urgence.

Un nouveau paragraphe 4 est ajouté à l'article 18/2 afin que ce soit clair qu'il existe trois régimes différents pour la mise en œuvre des BIM:

is overeenkomst de procedure beschreven in de door de Nationale Veiligheidsraad goedgekeurde geclassificeerde richtlijn van 25 maart 2019 betreffende het beroep op menselijke bronnen (zie p. 8 van de memorie van toelichting).

Zo kan de mogelijkheid om een BIM uit te voeren op een menselijke bron slechts worden gebruikt op een bron die geregistreerd is in de zin van artikel 3, 26° WIV en indien deze werd bevestigd door de inlichtingendienst waarmee hij samenwerkt. Die bevestiging houdt in dat de bron al meermaals intern werd geëvalueerd.

Door deze precisering wordt het onmogelijk om een BIM uit te voeren op een persoon die men overweegt als bron aan te werven, met als doel diens toegangen en diens contacten na te gaan, aangezien dit als overmatig en te ingrijpend in het privéleven werd beschouwd.

Art. 20

In artikel 18/2 wordt een verduidelijking toegevoegd om de procedures te standaardiseren:

zoals bepaald in artikel 18/10, § 4 (waarin de procedure wordt beschreven om in geval van hoogdringendheid een specifieke of uitzonderlijke methode voor het verzamelen van gegevens toe te passen) en de nieuwe artikelen 13/1 en 13/1/1 (het plegen van strafbare feiten door de agenten en de bronnen), kan de voorzitter van de Commissie, indien hij niet bereikbaar is, worden vervangen door een ander lid van de Commissie.

Voor het gebruik van een uitzonderlijke methode met betrekking tot een menselijke bron wordt geen aanpassing aangebracht aan het feit dat een ernstige potentiële bedreiging moet worden gerechtvaardigd overeenkomstig artikel 18/9 § 1, 1 ° en 2 ° (respectievelijk voor de VSSE en ADIV).

Om te antwoorden op de adviezen van de Raad van State (art. 19) en de BIM-Commissie (p.7) wordt het woord "gecontacteerd" weggelaten omdat, wanneer de voorzitter van de BIM-Commissie verhinderd is, een "ander lid" de voorzitters van de Ordes of de Vereniging van journalisten zal inlichten. Immers, in het kader van deze procedure wordt het lid van de BIM-Commissie, dat de verhinderde voorzitter van de BIM-Commissie vervangt, niet formeel "gecontacteerd", zoals dat het geval is bij de procedure van hoogdringendheid.

Een nieuwe paragraaf 4 wordt toegevoegd aan het artikel 18/2 om te verduidelijken dat er drie verschillende regelingen bestaan voor de uitvoering van BIM's:

— Les paragraphes 1er et 2 concernent les BIM effectuées sur des cibles;

— le paragraphe 3 vise le régime spécifique pour les professions protégées (avocat, médecin et journaliste);

— le nouveau paragraphe 4 prévoit les règles pour effectuer des BIM sur les sources humaines. Ainsi, certaines des mentions obligatoires pour demander une méthode spécifique ou exceptionnelle sont adaptées:

1) le code d'identification de la source sera repris dans la demande, à la place de son nom;

2) la menace potentielle qui doit être justifiée pour une BIM sur une cible n'est pas applicable pour une BIM sur une source. Dans ce cas, c'est le préjudice potentiel pour l'exercice des missions des services ou le danger potentiel pour la sécurité de la source humaine qui devra être démontrée. Les dérogations sont prévues respectivement aux articles 18/3 (pour les méthodes spécifiques) et 18/10 (pour les méthodes exceptionnelles).

Art. 21

Vu les modifications apportées aux articles 18 § 2 et 18/1, 3°, l'article 18/3 (qui prévoit la procédure en cas de méthode de recueil de données spécifique) est adapté.

Dans le paragraphe 1er, il est ajouté que, dans le cadre de l'article 18, § 2, la méthode spécifique doit être choisie en fonction du degré de gravité du préjudice potentiel pour l'exercice des missions des services ou du danger potentiel pour la sécurité de la source humaine.

Le paragraphe 2 est également adapté afin d'inclure que dans le cadre de l'article 18 § 2 et par dérogation à l'alinéa 1er, 2° et 3°, la décision du dirigeant du service mentionne le code d'identification de la source humaine. Ainsi, le véritable nom de la source n'est pas indiqué afin que son identité soit protégée, conformément à l'article 13 LRS.

Par ailleurs, le préjudice potentiel pour l'exercice des missions des services ou le danger potentiel pour la sécurité de la source humaine doit être mentionné à la place de la menace potentielle, au sens des articles 8 et 11 de la LRS.

Les mots "les faits susceptibles d'être qualifiés infractions" sont utilisés afin que la demande contienne les faits précis qui sont planifiés. Par contre, la qualification

— paragrafen 1 en 2 inzake de BIM's uitgevoerd op doelwitten;

— paragraaf 3 beoogt de specifieke regeling voor de beschermde beroepen (advocaat, arts en journalist);

— de nieuwe paragraaf 4 voorziet regels om BIM's op menselijke bronnen uit te voeren. Zo werden enkele verplichte vermeldingen voor de aanvraag van een specifieke of uitzonderlijke methode aangepast:

1) in de aanvraag wordt de identificatiecode van de bron vermeld in plaats van diens naam;

2) de potentiële dreiging die voor een BIM op een doelwit moet worden verantwoord, is niet van toepassing voor een BIM op een bron. In dat geval moeten het potentieel nadeel voor de uitoefening van de opdrachten van de diensten of het potentiële gevaar voor de veiligheid van de menselijke bron worden aangetoond. Er worden afwijkingen voorzien van de artikelen 18/3 (voor de specifieke methoden) en 18/10 (voor de uitzonderlijke methoden).

Art. 21

Gezien de wijzigingen aangebracht aan de artikelen 18 § 2 en 18/1, 3°, werd artikel 18/3 (dat de procedure voorziet in het geval van een specifieke methode van het verzamelen van inlichtingen) aangepast.

In de eerste paragraaf wordt toegevoegd dat, in het kader van artikel 18, § 2, de specifieke methode moet worden gekozen in functie van de graad van ernst van het potentieel nadeel voor de uitoefening van de opdrachten van de dienst of van het potentiële gevaar voor de veiligheid van de menselijke bron.

De tweede paragraaf wordt eveneens aangepast, zodat wordt opgenomen dat in het kader van artikel 18, § 2, en in afwijking van de eerste alinea, 2° en 3°, de beslissing van het diensthoofd de identificatiecode van de menselijke bron vermeldt. Zo wordt de echte naam van de bron niet vermeld, om diens identiteit te beschermen overeenkomstig artikel 13 WIV.

Tevens dient het potentieel nadeel voor de uitoefening van de opdrachten van de diensten of het potentiële gevaar voor de veiligheid van de menselijke bron te worden vermeld, in plaats van de potentiële bedreiging, in de zin van de artikelen 8 en 11 van de WIV.

De woorden "de feiten die als misdrijf kunnen gekwalificeerd worden" worden gebruikt opdat het verzoek de specifieke feiten die gepland zijn, omvat. Anderzijds wordt

elle-même, qui n'entre pas dans les compétences d'un service de renseignement, est laissée à l'appréciation de la Commission qui est composée de magistrats.

Pour tenir compte du point 8 de l'avis du Comité R, le concept d' "officier de renseignement" est remplacé aux paragraphes 2, 3 et 7 par l' "officier des méthodes" afin de faire correspondre le titre de cet agent avec l'évolution de ses compétences (voir article 2 du présent projet de loi).

Le paragraphe 6 est également légèrement adapté afin d'uniformiser le texte de la loi et ainsi utiliser les mêmes termes que ceux employés à l'article 18/10, § 6 de la LRS (méthode exceptionnelle).

La commission de la protection de la vie privée est remplacée par le Comité permanent R depuis l'entrée en vigueur de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Art. 22

Suite aux avis de la Commission BIM (pp. 5-6), du Comité R (points 59, 60, 63, 64, 65, 66) et du Collège des procureurs généraux, les auteurs du projet ont décidé d'insérer un nouvel article 18/5/1 dans la LRS pour créer une nouvelle méthode spécifique de recueil de données. Cette méthode vise l'infiltration avec une identité ou une qualité fictive dans le monde virtuel par un agent d'un service de renseignement.

En effet, lorsque l'agent utilise une identité ou une qualité fictive dans le cadre de son infiltration au sens de la nouvelle définition insérée à l'article 3, 27°, en vue de collecter des informations sur les personnes ciblées, les auteurs du projet ont estimé qu'un encadrement renforcé était nécessaire. Dans ce cas, c'est la nouvelle méthode spécifique de recueil de données (article 18/5/1) qui s'applique et non la méthode ordinaire (art. 16/5).

Par ailleurs, l'infiltration dans le "monde virtuel" se comprend *a contrario* de la signification de l'infiltration dans le monde réel énoncée dans la nouvelle méthode 18/12/1: c'est une infiltration où les relations se déroulent principalement avec des contacts physiques directs sans dissimuler son apparence physique.

On entend par exemple par "monde virtuel", un espace où les échanges se déroulent en utilisant des moyens de communication électronique.

de kwalificatie zelf, die niet onder de bevoegdheid van een inlichtingendienst valt, overgelaten aan het oordeel van de uit magistraten samengestelde Commissie.

Om rekening te houden met punt 8 van het advies van het Comité I wordt het begrip "inlichtingenofficier" in de paragrafen 2, 3 en 7 vervangen door "methodenofficier", zodat de titel van deze agent overeenstemt met de evolutie van zijn bevoegdheden (zie artikel 2 van het huidige wetsontwerp).

Paragraaf 6 wordt licht aangepast om de wettekst uniform te maken en dezelfde bewoording te hanteren als in artikel 18/10, § 6 van de WIV (uitzonderlijke methode).

De commissie voor de bescherming van de persoonlijke levenssfeer is vervangen door het Vast Comité I sinds de inwerkingtreding van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

Art. 22

Naar aanleiding van de adviezen van de BIM-Commissie (p. 5-6), van het Comité I (punten 59, 60, 63, 64, 65, 66) en van het College van procureurs-generaal, hebben de auteurs van het ontwerp besloten om een nieuw artikel 18/5/1 in te voegen in de WIV, dat een nieuwe specifieke inlichtingenmethode creëert. Deze methode beoogt de infiltratie in de virtuele wereld door een agent van de inlichtingendienst met een fictieve identiteit of hoedanigheid.

De auteurs van het ontwerp waren van oordeel, dat er inderdaad een sterkere omkadering nodig was, wanneer een agent een fictieve identiteit of hoedanigheid gebruikt, in het kader van diens infiltratie in de zin van de nieuwe definitie ingevoegd in artikel 3, 27° om informatie over geviseerde personen te verzamelen. In dit geval is de nieuwe specifieke methode voor het verzamelen van gegevens (artikel 18/5/1) van toepassing en niet de gewone methode (art. 16/5).

Anderzijds dient men infiltratie in de "virtuele wereld" te begrijpen als tegengesteld aan de betekenis van infiltratie in de echte wereld, zoals uiteengezet in de nieuwe methode 18/12/1: dat is een infiltratie waarbij de relaties hoofdzakelijk plaatsvinden via rechtstreekse fysieke contacten zonder dat daarbij zijn fysieke uiterlijk verborgen wordt.

Met "virtuele wereld" wordt bijvoorbeeld bedoeld een plek waar uitwisseling door middel van elektronische communicatie plaatsvindt.

Cela induit donc que le monde virtuel est celui où il n'y a pas de contact physique et/ou visuel direct (en présentiel) entre l'agent du service de renseignement et la cible.

Dès lors, une interaction par courrier électronique, messagerie cryptée, Vidéo conférence, forum, téléphone, courrier est considérée comme virtuelle.

Art. 23

Vu les modifications apportées aux articles 18, § 2 et 18/1, 3°, l'article 18/9 est adapté pour tenir compte de la procédure de mise en œuvre d'une méthode exceptionnelle de recueil de données.

Au paragraphe 1er, 1° et 2°, il est ainsi précisé que dans le cadre de l'article 18, § 2, une méthode exceptionnelle peut être mise en œuvre lorsqu'il existe un préjudice potentiel grave pour l'exercice des missions des services ou un danger potentiel grave pour la sécurité de la source humaine.

La reformulation proposée par le Conseil d'État (à l'article 21 de son avis) n'a dès lors pas été intégrée puisqu'on ne parle plus de menace potentielle grave.

Les paragraphes 2 et 3 ont également été adaptés pour inclure le préjudice ou le danger potentiel grave.

Art. 24

Vu les modifications apportées aux articles 18, § 2 et 18/1, 3°, l'article 18/10 (qui prévoit la procédure en cas de méthode de recueil de données exceptionnelle) est adapté.

Le paragraphe 2 (qui prévoit les mentions du projet d'autorisation) est également adapté afin d'inclure que dans le cadre de l'article 18 § 2 et par dérogation à l'alinéa 1er, 2° et 3°, la décision du dirigeant du service mentionne le code d'identification de la source humaine. Ainsi, le véritable nom de la source n'est pas indiqué afin que son identité soit protégée, conformément à l'article 13 LRS.

Par ailleurs, le préjudice potentiel grave pour l'exercice des missions des services ou le danger potentiel grave pour la sécurité de la source humaine doit être mentionné à la place de la menace potentielle grave, au sens des articles 8 et 11 de la LRS.

Dit brengt met zich mee dat de virtuele wereld de wereld is zonder fysiek en/of rechtstreeks (in aanwezigheid) visueel contact tussen de agent van de inlichtingendienst en het doelwit.

Hierdoor worden als virtueel beschouwd de interacties via e-mail, versleutelde berichtendienst, videoconferentie, forum, telefoon en post.

Art. 23

Gezien de wijzigingen aangebracht aan de artikelen 18, § 2 en 18/1, 3°, werd artikel 18/9 aangepast om rekening te houden in de procedure met het uitvoeren van een uitzonderlijke methode voor het verzamelen van inlichtingen.

Zo wordt in paragraaf 1, 1° en 2° verduidelijkt dat in het kader van artikel 18, § 2 een uitzonderlijke methode kan worden uitgevoerd, wanneer er een potentieel ernstig nadeel bestaat voor de uitoefening van de opdrachten van de diensten of een potentieel ernstig gevaar voor de veiligheid van de menselijke bron.

De herformulering die de Raad van State voorstelt (in artikel 21 van zijn advies) werd bijgevolg niet opgenomen, aangezien men niet meer spreekt over een potentieel ernstige dreiging.

De paragrafen 2 en 3 werden eveneens aangepast om het potentieel ernstig nadeel of het gevaar op te nemen.

Art. 24

Gezien de wijzigingen aangebracht aan de artikelen 18, § 2 en 18/1, 3°, werd artikel 18/10 (dat de procedure voorziet in het geval van een uitzonderlijke methode voor het verzamelen van inlichtingen) aangepast.

Paragraaf 2 (dat de vermeldingen van het ontwerp van machtiging voorziet) wordt ook aangepast, om op te nemen dat in het kader van artikel 18, § 2, en in afwijking van alinea 1, 2° en 3°, de beslissing van het diensthoofd de identificatiecode van de menselijke bron vermeldt. Op die manier wordt de echte naam van de bron niet aangeduid, zodat diens identiteit wordt beschermd overeenkomstig artikel 13 WIV.

Het potentieel ernstig nadeel voor de uitoefening van de opdrachten van de diensten of het potentieel ernstig gevaar voor de veiligheid van de menselijke bron dienen te worden vermeld, in plaats van de potentieel ernstige bedreiging, in de zin van de artikelen 8 en 11 van de WIV.

Pour tenir compte du point 8 de l'avis du Comité R, le concept d' "officier de renseignement" est remplacé aux paragraphes 1er , 2, 6° et 4 par l' "officier des méthodes" afin de faire correspondre le titre de cet agent avec l'évolution de ses compétences (voir article 2 du présent projet de loi).

Les mots "les faits susceptibles d'être qualifiés infractions" sont utilisés afin que la demande contienne les faits précis qui sont planifiés. Par contre, la qualification elle-même, qui n'entre pas dans les compétences d'un service de renseignement, est laissée à l'appréciation de la Commission qui est composée de magistrats.

Une précision est ajoutée pour uniformiser les procédures:

comme prévu à l'article 18/10 § 4 (qui décrit la procédure en cas d'extrême urgence pour effectuer une méthode spécifique ou exceptionnelle de recueil de données) et les nouveaux articles 13/1 et 13/1/1 (commission d'infractions par les agents et les sources), lorsque le président de la Commission n'est pas joignable, il peut être remplacé par un autre membre de la Commission.

La commission de la protection de la vie privée est remplacée par le Comité permanent R depuis l'entrée en vigueur de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Art. 25 (nouvel art. 18/12/1)

Nécessité d'un nouvel article sur l'infiltration dans le monde réel

En 2016, lors du projet de loi qui a introduit l'article 13/2 dans la LRS, le gouvernement a précisé que cette nouvelle mesure d'appui ne constituait pas la base légale pour faire de l'infiltration car les garanties adéquates n'étaient pas mises en place.

Depuis 2016, le contexte a cependant changé, comme l'ont reconnu la Commission d'enquête parlementaire et l'accord de gouvernement.

En effet, cette nécessité faisait l'objet d'une recommandation de la Commission d'enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016, dans son troisième rapport intermédiaire sur le volet "architecture de la sécurité": "La loi du 30 mars 2017 prévoit certes une extension des possibilités, pour les agents de la VSSE, d'intervenir sous une identité ou une qualité

Om rekening te houden met punt 8 van het advies van het Comité I wordt het begrip "inlichtingenofficier" in de paragrafen 1, 2, 6° en 4 vervangen door "methodenofficier", zodat de titel van deze agent overeenstemt met de evolutie van zijn bevoegdheden (zie artikel 2 van het huidige wetsontwerp).

De woorden "de feiten die als misdrijf kunnen gekwalificeerd worden" worden gebruikt opdat het verzoek de specifieke feiten die gepland zijn, omvat. Anderzijds wordt de kwalificatie zelf, die niet onder de bevoegdheid van een inlichtingendienst valt, overgelaten aan het oordeel van de uit magistraten samengestelde Commissie.

Een verduidelijking wordt toegevoegd om de procedures te standaardiseren:

zoals bepaald in artikel 18/10, § 4 (waarin de procedure wordt beschreven om in geval van hoogdringendheid een specifieke of uitzonderlijke methode voor het verzamelen van gegevens toe te passen) en de nieuwe artikelen 13/1 en 13/1/1 (het plegen van strafbare feiten door de agenten en de bronnen), kan de voorzitter van de Commissie, wanneer die niet bereikbaar is, worden vervangen door een ander lid van de Commissie.

De commissie voor de bescherming van de persoonlijke levenssfeer is vervangen door het Vast Comité I sinds de inwerkingtreding van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

Art. 25 (nieuw art. 18/12/1)

Noodzaak aan een nieuw artikel over de infiltratie in de echte wereld.

In 2016 heeft de regering, naar aanleiding van het wetsontwerp waarbij artikel 13/2 in de WIV werd ingevoerd, verduidelijkt dat deze nieuwe ondersteuningsmaatregel geen wettelijke basis vormde om aan infiltratie te doen, omdat de gepaste waarborgen niet werden ingebouwd.

Sinds 2016 is de context echter veranderd, zoals de parlementaire onderzoekscommissie en het regeerakkoord hebben erkend.

De parlementaire onderzoekscommissie belast met het onderzoek naar de omstandigheden die hebben geleid tot de terroristische aanslagen van 22 maart 2016, deed deze aanbeveling inderdaad reeds in haar derde tussentijdse verslag over het onderdeel "veiligheidsarchitectuur": "De wet van 30 maart 2017 voorziet weliswaar een uitbreiding van de mogelijkheden voor agenten van de VSSE om onder een fictieve identiteit of

fictives, mais elle ne les autorise pas à organiser de véritables opérations d'infiltration, au cours desquelles ces agents seraient amenés à infiltrer durablement un milieu donné. Eu égard à la nécessité de renforcer la position d'information de la VSSE, la commission d'enquête juge souhaitable d'autoriser l'infiltration dans le cadre de la mission de renseignement. La réglementation légale à adopter en la matière devra toutefois prévoir les garanties nécessaires, tant en termes de protection juridique des citoyens qu'en termes de sécurité des agents de la VSSE chargés de missions d'infiltration."

Cette nécessité a été réaffirmée dans l'accord de gouvernement: "La position d'information des services de renseignement et de l'OCAM sera renforcée. Un cadre légal adapté concernant l'infiltration d'agents et d'informateurs, ainsi que pour le contrôle des sources, sera mis en place."

Comme expliqué ci-dessus, les précautions prises par un nombre croissant d'individus qui présentent une menace pour la sécurité nationale rend la tâche des services de renseignement de plus en plus compliquée. Il n'est pas rare que des méthodes, pourtant intrusives, ne permettent pas d'évaluer avec suffisamment d'acuité la dangerosité, les intentions d'un individu ou même de l'identifier formellement, notamment lorsqu'il utilise des pseudonymes virtuels. Il n'est parfois pas non plus possible de déployer une source humaine (HUMINT) au contact dudit individu sans éveiller sa suspicion et mettre en danger la source.

Dans ce contexte, il devient indispensable que, dans le monde réel également, les agents des services de renseignement et de sécurité aient la possibilité de s'infiltrer afin de s'intégrer dans un groupe ou dans la vie d'une personne présentant une menace pour la sécurité nationale et qui fait donc l'objet d'une enquête d'un service de renseignement et de sécurité.

C'est ainsi que suite aux avis de la Commission BIM (pp. 5-6), du Comité R (points 48, 59, 60, 63, 64, 65) et du Collège des procureurs généraux, les auteurs du projet ont décidé d'insérer un nouvel article 18/12/1 dans la loi pour créer une nouvelle méthode exceptionnelle de recueil de données. Cette méthode vise l'infiltration dans le monde réel d'un agent qui dissimule sa qualité d'agent d'un service de renseignement, et pour les agents du SGRS, également de membre de la Défense.

hoedanigheid op te treden, doch biedt geen grondslag voor het opzetten van werkelijke infiltratieoperaties, waarbij deze agenten op een duurzame wijze in een bepaald milieu zouden binnendringen. Met het oog op de noodzakelijke versterking van de informatiepositie van de VSSE acht de onderzoekscommissie de bevoegdheid tot infiltratie in het kader van een inlichtingenopdracht wenselijk. In de uit te werken wettelijke regeling moeten echter de nodige waarborgen worden voorzien, zowel inzake de rechtsbescherming van de burgers als inzake de veiligheid van de agenten van de VSSE die met de infiltratie worden belast."

Deze noodzaak werd nogmaals bevestigd in het regeerakkoord: "De informatiepositie van inlichtingendiensten en het OCAD wordt versterkt. Een aangepast wettelijk kader voor infiltratie door agenten en informanten wordt gecreëerd. Dit gebeurt ook voor het toezicht op de bronnen."

Zoals hierboven werd uiteengezet, maken de voorzorgsmaatregelen genomen door een groeiend aantal individuen die een bedreiging vormen voor de nationale veiligheid, de taak van de inlichtingendiensten steeds ingewikkelder. Het is niet ongewoon dat zelfs ingrijpende methoden niet toelaten om een voldoende nauwkeurige beoordeling te verkrijgen van de gevaarlijkheid, de bedoelingen van een persoon of om hem alleen nog maar formeel te identificeren, met name wanneer hij virtuele pseudoniemen gebruikt. Het is soms eveneens onmogelijk om een menselijke bron (HUMINT) in te zetten die in contact staat met de genoemde persoon, zonder diens wantrouwen op te wekken en de bron in gevaar te brengen.

In deze context wordt het noodzakelijk dat de agenten van de inlichtingen- en veiligheidsdiensten zelf in de echte wereld kunnen infiltreren, om zich te integreren in een groep of in het leven van een persoon die een bedreiging vormen voor de nationale veiligheid en die dus het voorwerp uitmaken van een onderzoek van een inlichtingen- en veiligheidsdienst.

Het is om die reden, en naar aanleiding van de adviezen van de BIM-Commissie (p. 5-6) en van het Comité I (punten 48, 59, 60, 63, 64, 65) en van het College van procureurs-generaal, dat de auteurs van het ontwerp besloten om een nieuw artikel 18/12/1 in de wet op te nemen, dat een nieuwe uitzonderlijke methode voor het verzamelen van gegevens creëert. Deze methode beoogt de infiltratie in de echte wereld door een agent die zijn hoedanigheid van agent van een inlichtingendienst, en voor de agenten van ADIV ook van lid van Defensie, verbergt.

Les auteurs du projet estiment que l'infiltration, dans le monde réel, dans un milieu visé par une enquête d'un service de renseignement et de sécurité et souvent dangereux, est une action délicate qu'il convient de contrôler de manière renforcée. En effet, il s'agit alors d'une opération comportant des risques importants pour l'agent infiltré et impliquant une atteinte à la vie privée.

Une infiltration dans le monde réel est donc une infiltration (au sens du point 27° de l'article 3) où les relations se déroulent principalement avec des contacts physiques directs et où on ne peut pas dissimuler son apparence physique.

Pour rappel, l'infiltration (art. 3, 27°) est définie comme suit:

"le fait pour un agent, en dehors des cas visés à l'article 18, de s'intégrer délibérément dans un groupe ou dans la vie d'une personne afin de recueillir des informations ou des données, dans le cadre d'une enquête d'un service de renseignement et de sécurité et dans l'intérêt de l'exercice de ses missions. Cet agent dissimule sa qualité d'agent des services de renseignement et de sécurité et, pour les agents du Service Général du Renseignement et de la Sécurité, de membre du ministère de la Défense, et:

a) participe ou facilite les activités ou soutient activement les convictions ou les activités de la personne ou du groupe qui fait l'objet de l'enquête, ou

b) entretient des relations durables avec ceux-ci."

Par ailleurs, vu la complexité des questions relatives à la mise en place d'une telle méthode et de la nature hautement sensible des informations qui entourent une telle procédure, les auteurs du projet ont prévu qu'une directive classifiée et validée par le Conseil National de Sécurité serait rédigée afin de déterminer les modalités d'application pratiques de l'infiltration dans le monde réel. Pour répondre au point 61 de l'avis du Comité R, la notion de "relations durables" et tout autre terme devant l'être pour des raisons opérationnelles seront ainsi précisés dans cette directive.

En outre, vu l'investissement préalable important pour mettre en place ce type de méthode, à l'instar de la méthode exceptionnelle de recours à des personnes morales (art. 18/13), les services de renseignement peuvent obtenir l'autorisation de procéder à une infiltration aussi longtemps qu'elle est nécessaire aux finalités pour lesquelles elle est mise en œuvre (voir point 66 de l'avis du Comité R). Le service de renseignement et de sécurité concerné fait rapport à la Commission tous les

De auteurs van het ontwerp zijn van mening dat de infiltratie in de echte wereld, in een door een inlichtingen- en veiligheidsdienst geviseerd en vaak gevaarlijk milieu, een delicate handeling is die strenger gecontroleerd dient te worden. Het gaat immers om een operatie die belangrijke risico's inhoudt voor de infiltrerende agent en een inbreuk in het privéleven veronderstelt.

Een infiltratie in de echte wereld, is dus een infiltratie (in de zin van punt 27° van artikel 3) waarbij de relaties hoofdzakelijk plaatsvinden via rechtstreekse fysieke contacten, en waarbij het fysieke uiterlijk niet kan worden verborgen.

Ter herinnering, infiltratie (art. 3, 27°) wordt gedefinieerd als:

"het feit dat een agent, buiten de gevallen bedoeld in artikel 18, zich doelbewust in een groep of in het leven van een persoon integreert om informatie of gegevens te verzamelen, in het kader van een onderzoek door een inlichtingen- en veiligheidsdienst en in het belang van de uitoefening van zijn opdrachten. Deze agent verbergt zijn hoedanigheid van agent van de inlichtingen- en veiligheidsdiensten, en voor de agenten van de Algemene Dienst Inlichtingen en Veiligheid, van lid van het ministerie van Defensie, en:

a) hij neemt deel aan activiteiten of maakt ze mogelijk, of hij ondersteunt actief de overtuigingen of de activiteiten van de persoon of de groep die het voorwerp uitmaakt van het onderzoek, of

b) hij onderhoudt duurzame relaties met hen"

Bovendien, gelet op de complexe vragen bij het inzetten van zo'n methode en de van nature hoogst gevoelige informatie die in deze procedure omgaat, hebben de auteurs van dit ontwerp voorzien om een geclassificeerde richtlijn op te stellen, gevalideerd door de Nationale Veiligheidsraad, om de toepassingsmodaliteiten van de infiltratie in de echte wereld vast te leggen. In antwoord op het punt 61 van het advies van het Comité I, worden het begrip "duurzame relaties" en alle begrippen die nodig zijn voor de operaties gepreciseerd in deze richtlijn.

Gelet op de belangrijke investering vooraf die nodig is om dit type van methode uit te voeren, zoals voor de uitzonderlijke methode om een rechtspersoon in te zetten (art. 18/13), kunnen de inlichtingendiensten een machtiging voor een infiltratie verkrijgen, voor zolang als nodig is voor het doel waarvoor ze wordt aangewend (zie punt 66 van het advies van het Comité I). De betrokken inlichtingen- en veiligheidsdienst brengt om de twee maanden verslag uit aan de Commissie over de evolutie

deux mois sur l'évolution de la menace qui a nécessité le recours à l'infiltration dans le monde réel.

Bien entendu, si la Commission estime que la période demandée est disproportionnée, elle ne donnera qu'un accord partiel, donc sur une durée limitée.

Dans le cadre de la procédure prévue pour les méthodes exceptionnelles visée à l'article 18/10 § 7 de la loi, la Commission transmet tous les documents en lien avec la méthode au Comité R afin que ce dernier puisse exercer utilement son contrôle. La Commission peut à tout moment mettre un terme à l'utilisation de la méthode.

De plus, une procédure interne avec plusieurs niveaux de validation sera mise en place afin d'élaborer la demande d'autorisation d'utiliser cette nouvelle méthode pour collecter des données par l'équipe ou l'agent responsable, avant d'être introduite auprès du dirigeant du service concerné.

Exemple illustrant la nécessité de devoir obtenir une autorisation sur une longue période:

Un agent d'un service de renseignement étranger est actif en Belgique sous couverture officielle. Celui-ci est particulièrement vigilant par rapport aux communications téléphoniques et électroniques qu'il utilise. Afin de pouvoir obtenir des informations sur les activités, les points d'intérêts ou de faiblesse de l'agent de renseignement étranger, un agent d'un service de renseignement et de sécurité belge va, de manière durable, socialiser avec celui-ci à l'occasion d'événements culturels et/ou sportifs. Pour cela, l'agent de renseignement belge devra utiliser une identité fictive afin de s'inscrire dans des clubs ou des associations, effectuer les paiements liés à ces activités, recevoir les invitations et pour finalement entrer en contact avec l'agent de renseignement étranger. Il devra entretenir cette relation sur le long terme vu que certains agents de renseignement étrangers sont en mission en Belgique durant plusieurs années et partager ses convictions pour développer une relation de confiance.

En outre, l'agent infiltré devra dissimuler sa qualité d'agent d'un service de renseignement belge, soit en utilisant une identité ou une qualité fictive (telle que définies à l'article 3, 24° et 25°) soit en ayant recours à un faux nom ou une fausse qualité.

Les auteurs du projet de loi rappellent que dissimuler la qualité d'agent d'un service de renseignement est, en cas d'infiltration, indispensable. Cela permet de mieux assurer la sécurité de l'agent en évitant que le lien soit directement établi avec un service de renseignement et

van de dreiging die het beroep op een infiltratie in de echte wereld noodzakelijk maakte.

Indien de Commissie van oordeel is dat de gevraagde periode onevenredig is, zal zij slechts een gedeeltelijk akkoord geven, d.w.z. voor een beperkte duur.

In het kader van de procedure voorzien voor de uitzonderlijke methoden bedoeld in artikel 18/10, § 7 van de wet, maakt de Commissie alle documenten in verband met de methode over aan het Comité I, zodat deze laatste zijn controle naar behoren kan uitoefenen.De Commissie kan te allen tijde een eind maken aan het gebruik van de methode.

Bovendien, zal er een interne procedure met verschillende validatieniveaus worden ingevoerd waarbij het verantwoordelijke team of de verantwoordelijke agent de aanvraag moet uitwerken om een fictieve identiteit te mogen gebruiken om informatie te verzamelen

Voorbeeld waaruit blijkt dat de toestemming voor een lange periode moet worden verkregen:

Een agent van een buitenlandse inlichtingendienst is in België actief onder een officiële dekmantel. Hij is bijzonder waakzaam met betrekking tot zijn telefonische en elektronische communicatie. Om informatie over de activiteiten, interesses of zwakke punten van de buitenlandse inlichtingenagent te verkrijgen, zal een agent van een Belgische inlichtingen- en veiligheidsdienst duurzaam met hem socializen op culturele en/of sportieve evenementen. Daartoe zal de Belgische inlichtingenagent een fictieve identiteit moeten gebruiken om zich in te schrijven in clubs of verenigingen, om betalingen in verband met die activiteiten te doen, om uitnodigingen te ontvangen en tot slot om in contact te treden met de buitenlandse inlichtingenagent. Hij zal die relatie op lange termijn moeten onderhouden, aangezien bepaalde buitenlandse inlichtingenagenten voor meerdere jaren in België op missie worden gestuurd, en zijn overtuigingen moeten delen om een vertrouwensrelatie op te bouwen.

Daarnaast zal de infiltrerende agent zijn hoedanigheid van agent van een Belgische inlichtingendienst moeten verbergen, hetzij door een fictieve identiteit of hoedanigheid te gebruiken (zoals gedefinieerd in artikel 3, 24° en 25°), hetzij door middel van een valse naam of een valse hoedanigheid.

De auteurs van het wetsontwerp herinneren eraan dat de hoedanigheid van agent van een inlichtingendienst kunnen verbergen, onontbeerlijk is bij een infiltratie. Het laat toe om de veiligheid van de agent beter te waarborgen, door te vermijden dat er een rechtstreeks

une liste éventuelle d'agents. La position de l'agent, qui s'apprête à entrer et s'intégrer dans un environnement dangereux, est ainsi plus efficacement protégée. Le cas échéant, l'utilisation d'une identité fictive, appuyée par des documents officiels (permis de conduire fictif, carte d'identité fictive, etc.) sera nécessaire pour protéger correctement cet agent et renforcer sa crédibilité vis-à-vis de la cible afin d'obtenir les informations nécessaires à l'exercice de ses missions.

Par ailleurs, les auteurs du texte n'ont pas jugé utile d'insérer la dérogation précisée à l'article 18/4, § 3 et 18/11, § 3 comme suggérée par le Comité R dans son avis (point 66, 2e tiret) vu la refonte complète de cet article.

Art. 26

Cet article prévoit des adaptations à l'article 18/15 de la LRS.

Une disposition similaire à celle de l'article 46*quater* du Code d'instruction criminelle a déjà été reprise à l'article 18/15 de la LRS, introduite par la loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité (*MB* 10 mars 2010).

La loi du 4 février 2010 (dite "loi BIM") a étendu les compétences des services de renseignement et de sécurité en matière d'enquête dans le cadre de l'exercice de leur mission légale de renseignement et les a réparties en trois catégories: les méthodes ordinaires, les méthodes spécifiques et les méthodes exceptionnelles de recueil des données (cf. articles 14 à 18/7 de la LRS). Cette répartition légale en trois catégories repose sur le degré d'intrusion d'une méthode dans la vie privée des citoyens (exceptionnelle = degré le plus élevé; spécifique = moyen, ordinaire = limité à très limité), ce degré étant lui-même déterminé tant par la nature des données recueillies que par la manière dont les données sont recueillies. Des conditions d'application générale, des procédures et des mécanismes de contrôle spécifiques ont été définis pour chaque catégorie de méthode de renseignement. Le champ d'application du présent article 18/15 de la LRS, qui relève des méthodes exceptionnelles, se fonde sur le champ d'application de l'article 46*quater* du Code d'instruction criminelle, défini par la loi du 27 décembre 2005.

A l'instar de l'article 46*quater* du Code d'instruction criminelle, il convient de modifier l'article 18/15 de la LRS.

verband wordt gelegd met een inlichtingendienst en een lijst van mogelijke agenten. De positie van de agent, die op het punt staat zich in een gevaarlijk milieu te integreren, wordt op die manier doeltreffender beschermd. In voorkomend geval moet het gebruik van een fictieve identiteit, die wordt ondersteund door officiële documenten (fictief rijbewijs, fictieve identiteitskaart, …), de agent op correcte wijze beschermen en diens geloofwaardigheid ten opzichte van het doelwit vergroten om zo de noodzakelijke informatie te verkrijgen in de uitoefening van zijn opdrachten.

De auteurs van de tekst achtten het daarentegen niet nuttig om de afwijking van artikel 18/4, § 3 en 18/11, § 3 op te nemen, zoals het Comité I in zijn verslag voorstelt (punt 66, 2e streepje), aangezien het artikel volledig wordt herzien.

Art. 26

Dit artikel voorziet in aanpassingen aan artikel 18/15 WIV.

Een gelijkaardige bepaling zoals in artikel 46*quater* Sv. is reeds opgenomen in artikel 18/15 van de WIV, ingevoerd met de wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten (*BS* 10 maart 2010).

De wet van 4 februari 2010 (de zogenoemde BIM-wet) breidde de onderzoeksbevoegdheden van de inlichtingen- en veiligheidsdiensten binnen het uitoefenen van de wettelijke inlichtingenopdracht uit, en deelde ze in drie categorieën in, zijnde de gewone, de specifieke en de uitzonderlijke methoden voor het verzamelen van gegevens (cf. artikelen 14 tot 18/17 WIV). Deze wettelijke drieledige indeling is gebaseerd op de graad van de inmenging die een methode kan teweegbrengen in de persoonlijke levenssfeer van de burger (uitzonderlijk = meeste inmenging in privacy; specifiek = minder; gewoon = weinig tot zeer weinig), waarbij deze graad op zijn beurt bepaald wordt door zowel de aard van de ingewonnen gegevens als de manier waarop de gegevens ingewonnen worden. Elke categorie van inlichtingenmethoden heeft zijn eigen algemene toepassingsvoorwaarden, procedures en controlemechanismen. Het toepassingsgebied van het huidige artikel 18/15 WIV, die behoort tot de uitzonderlijke methoden, is gebaseerd op het toepassingsgebied van artikel 46*quater* Sv zoals bepaald in de wet van 27 december 2005.

Artikel 18/15 WIV heeft eenzelfde behoefte tot aanpassing als artikel 46*quater* Sv.

Comme auparavant, le dirigeant du service de renseignement et de sécurité concerné (cf. article 18/9, § 2, alinéa 2, de la LRS) reste l'autorité compétente. Il s'agit plus particulièrement de l'administrateur général de la Sûreté de l'État et du chef du Service Général du Renseignement et de la Sécurité (cf. article 3, 8°, de la LRS).

Outre l'autorité compétente, les conditions d'application, la procédure et les mécanismes de contrôle externe demeurent également inchangés. Les articles 18/9 et 18/10 de la LRS en fournissent une description générale pour toutes les méthodes exceptionnelles. Concernant la compétence visée à l'article 18/15 de la LRS, les conditions cumulatives préliminaires suivantes sont applicables:

— une menace potentielle grave pour les intérêts fondamentaux du pays. En ce qui concerne la Sûreté de l'État, les intérêts à sauvegarder sont précisés à l'article 8, 2° à 4°, de la LRS et les menaces à combattre à l'article 8, 1°, de la LRS. Pour le Service Général du Renseignement et de la Sécurité, les intérêts à sauvegarder et les menaces à combattre sont mentionnés à l'article 11, § 1er, 1° à 3° et 5°, de la LRS;

— le principe de subsidiarité: lorsque les méthodes ordinaires et spécifiques sont jugées insuffisantes pour recueillir les informations nécessaires à l'aboutissement de la mission de renseignement;

— le principe de proportionnalité: la correspondance entre la nature de la méthode et le degré de gravité de la menace potentielle;

— une autorisation écrite et motivée du dirigeant du service;

— et l'avis conforme préalable de la Commission BIM.

En outre, il convient également de tenir compte de l'exigence selon laquelle le projet d'autorisation du dirigeant du service, soumis à la Commission BIM pour avis, doit mentionner un certain nombre d'éléments, sous peine d'illégalité:

1° la nature de la méthode exceptionnelle;

2° selon le cas, la ou les personnes physiques ou morales, les associations ou les groupements, les objets, les lieux, les événements ou les informations faisant l'objet de la méthode exceptionnelle;

3° la menace potentielle grave qui justifie la méthode exceptionnelle de recueil des données;

De bevoegde overheid blijft, zoals voorheen, het diensthoofd van de betrokken inlichtingen- en veiligheidsdienst (*cf.* artikel 18/9, § 2, tweede lid WIV). Meer bepaald is dit de administrateur-generaal van de Veiligheid van de Staat en de chef van de Algemene Dienst Inlichting en Veiligheid bij de Krijgsmacht (*cf.* artikel 3, 8° WIV).

Naast de bevoegde overheid, wordt ook aan de toepassingsvoorwaarden, de procedure en de externe controlemechanismen niet geraakt. Deze worden voor alle uitzonderlijke methoden op algemene wijze beschreven in de artikelen 18/9 en 18/10 WIV. Voor de bevoegdheid bedoeld in artikel 18/15 WIV gelden bijgevolg volgende cumulatieve preliminaire voorwaarden:

— een ernstige potentiële dreiging tegen de fundamentele belangen van het land. Voor wat betreft de Veiligheid van de Staat worden de te beschermen belangen omschreven in de artikel 8, 2° tot 4° WIV en de te bestrijden dreigingen in artikel 8, 1° WIV. Voor wat betreft de Algemene Dienst Inlichting en Veiligheid zijn de te beschermen belangen en de te bestrijden dreigingen omschreven in de artikel 11, § 1, 1° tot 3° en 5° WIV;

— het subsidiariteitsprincipe, zijnde de ontoereikendheid van de gewone en de specifieke methoden om de informatie te verzamelen die nodig is om de inlichtingenopdracht te volbrengen;

— het proportionaliteitsprincipe, zijnde het corresponderen van de aard van de methode met de graad van de ernst van de potentiële dreiging;

— een schriftelijke en gemotiveerde machtiging van het diensthoofd;

— een aan deze machtiging voorafgaand eensluidend advies van de BIM-Commissie.

Daarnaast moet ook rekening gehouden worden met de vereiste dat het ontwerp van machtiging van het diensthoofd, dat voor advies voorgelegd wordt aan de BIM-Commissie, een aantal op straffe van onwettigheid voorgeschreven vermeldingen moet bevatten:

1° de aard van de uitzonderlijke methode;

2° naargelang het geval, de natuurlijke personen of rechtspersonen, feitelijke verenigingen of groeperingen, voorwerpen, plaatsen, gebeurtenissen of informatie die het voorwerp uitmaken van de uitzonderlijke methode;

3° de ernstige potentiële dreiging die de uitzonderlijke methode voor het verzamelen van gegevens rechtvaardigt;

4° les circonstances de fait qui justifient la méthode exceptionnelle, la motivation en matière de subsidiarité et de proportionnalité, en ce compris le lien entre les dispositions reprises aux points 2° et 3°;

5° la période pendant laquelle la méthode exceptionnelle de recueil de données peut être pratiquée à compter de l'autorisation du dirigeant du service;

6° le nom de l'officier ou des officiers de renseignement chargé(s) du suivi la mise en œuvre de la méthode exceptionnelle;

7° le cas échéant, le moyen technique employé pour mettre en œuvre la méthode exceptionnelle en application des articles 18/11 ou 18/12;

8° le cas échéant, le concours avec une information ou une instruction judiciaire;

9° le cas échéant, les infractions strictement nécessaires afin d'assurer l'efficacité de la méthode ou de garantir la sécurité des agents ou de tiers;

10° le cas échéant, les indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle;

11° le cas échéant, les motifs qui justifient l'extrême urgence;

12° la date de l'autorisation;

13° la signature du dirigeant du service.

La durée d'une méthode exceptionnelle, et donc également la compétence d'enquête visée à l'article 18/15 de la LRS, ne peut excéder deux mois à compter de l'autorisation du dirigeant du service (cf. art. 18/10, § 1er de la LRS, deuxième alinéa). Une prolongation est possible, moyennant avis conforme préalable de la Commission BIM. Une seconde prolongation et toute nouvelle prolongation de la méthode n'est possible qu'en présence de circonstances particulières nécessitant de prolonger l'utilisation de cette méthode (cf. art. 18/10, § 5 de la LRS).

La première adaptation de l'article 18/15 de la LRS s'inscrit dans le prolongement de l'adaptation de l'article 46*quater* du Code d'instruction criminelle. L'énumération actuelle des données à requérir, limitative et incomplète, est remplacée par:

4° de feitelijke omstandigheden die de uitzonderlijke methode rechtvaardigen, de motivering inzake subsidiariteit en proportionaliteit, inbegrepen het verband tussen de bepalingen onder 2° en 3°;

5° de periode waarin de uitzonderlijke methode voor het verzamelen van gegevens kan worden aangewend, te rekenen vanaf de machtiging van het diensthoofd;

6° de naam van de inlichtingenofficier(en) verantwoordelijk om de aanwending van de uitzonderlijke methode op te volgen;

7° in voorkomend geval, het technisch middel dat gebruikt wordt bij de aanwending van de uitzonderlijke methode in toepassing van de artikelen 18/11 of 18/12;

8° in voorkomend geval, de samenloop met een opsporings- of gerechtelijk onderzoek;

9° in voorkomend geval, de strafbare feiten die strikt noodzakelijk zijn voor het welslagen van de uitvoering van de methode of ter verzekering van de veiligheid van de agenten of derden;

10° in voorkomend geval, de ernstige aanwijzingen waaruit blijkt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of de ontwikkeling van de potentiële dreiging;

11° in voorkomend geval, de redenen die de hoogdringendheid rechtvaardigen;

12° de datum van de machtiging;

13° de handtekening van het diensthoofd.

Een uitzonderlijke methode, en zodoende ook de onderzoeksbevoegdheid bedoeld in artikel 18/15 WIV, mag niet langer duren dan twee maanden te rekenen vanaf de machtiging van het diensthoofd (cf. art. 18/10, § 1, tweede lid WIV). Verlenging is mogelijk, mits voorafgaand eensluidend advies van de BIM-Commissie. Een tweede en elke volgende verlenging van een uitzonderlijke methode is slechts mogelijk indien er bijzondere omstandigheden aanwezig zijn die de verlenging van het gebruik van deze methode noodzaken (cf. art. 18/10, § 5 WIV).

De eerste aanpassing van artikel 18/15 WIV ligt in de lijn van de aanpassing van artikel 46*quater* Sv. De actuele, limitatieve en onvolledige opsomming van te vorderen gegevens wordt vervangen door:

— un renvoi à l'article 5, § 1er, 3° à 22°, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, qui permet de couvrir l'ensemble du secteur financier, des institutions non financières et des personnes intervenant dans des opérations financières;

— un renvoi aux gestionnaires de valeurs virtuelles et aux personnes et institutions facilitant les transactions incluant des valeurs virtuelles qui offrent leurs services sur le territoire belge, quel que soit leur lieu d'établissement.

Cela vaut de ce fait également pour les services, produits et instruments qui ne sont pas réglementés légalement, ou qui sont réglementés légalement mais sont offerts sans autorisation ou qui sont nouveaux et innovants.

Dans l'exercice de leur compétence d'enquête visée à l'article 18/15 de la LRS, le cadre strict de l'article 13 de la LRS, qui définit le traitement des informations et des données personnelles dans les services de renseignement et de sécurité, reste applicable en toute logique. Cette disposition prévoit que:

"Les services de renseignement et de sécurité peuvent rechercher, collecter, recevoir et traiter des informations et des données à caractère personnel qui peuvent être utiles à l'exécution de leurs missions et tenir à jour une documentation relative notamment à des événements, à des groupements et à des personnes présentant un intérêt pour l'exécution de leurs missions.

Les renseignements contenus dans la documentation doivent présenter un lien avec la finalité du fichier et se limiter aux exigences qui en découlent."

Une deuxième adaptation et une troisième adaptation de l'article 18/15 de la LRS devraient permettre une plus grande adéquation entre cette disposition et l'article 46*quater* du Code d'instruction criminelle.

La loi-programme du 1er juillet 2016 (*MB* du 4 juillet 2016) a conféré au ministère public un droit d'accès légal au Point de Contact Central de la Banque nationale de Belgique (PCC), initialement introduit par l'article 322, § 3, alinéa 1er, du Code des impôts sur les revenus 1992, pour obtenir les informations visées à l'article 46*quater*, § 1er, alinéa 1er, du Code d'instruction criminelle. Les services de renseignement et de sécurité disposent également chacun d'un droit d'accès, sur base d'une lecture combinée de l'article 14, deuxième alinéa et de l'article 18/15 LRS. Les modalités de ce droit d'accès

— een verwijzing naar artikel 5, § 1, 3° tot 22° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten, waarmee de gehele financiële sector en de niet-financiële instellingen en personen die tussenkomen bij financiële verrichtingen gevat worden;

— een verwijzing naar de beheerders van virtuele waarden en de personen en instellingen die transacties met virtuele waarden faciliteren, die hun diensten binnen het Belgische grondgebied ter beschikking stellen, ongeacht hun vestiging.

Hierdoor is het tevens van toepassing op diensten, producten en instrumenten die niet wettelijk geregeld zijn, die wel wettelijk geregeld zijn maar zonder vergunning worden aangeboden of die nieuw en innovatief zijn.

Bij de uitoefening van de onderzoeksbevoegdheid bedoeld in artikel 18/15 WIV blijft logischerwijs het strikte kader van artikel 13 WIV, dat de verwerking van informatie en persoonsgegevens bij de inlichtingen- en veiligheidsdiensten vastlegt, onverminderd gelden. Deze bepaling stelt:

"De inlichtingen- en veiligheidsdiensten kunnen informatie en persoonsgegevens opsporen, verzamelen, ontvangen en verwerken die nuttig kunnen zijn om hun opdrachten te vervullen en een documentatie bijhouden, meer bepaald met betrekking tot de gebeurtenissen, de groeperingen en de personen die een belang vertonen voor de uitoefening van hun opdrachten.

De in de documentatie vervatte inlichtingen moeten in verband staan met de doeleinden van het gegevensbestand en beperkt blijven tot de vereisten die eruit voortvloeien."

Een tweede en derde aanpassing van artikel 18/15 WIV dienen deze bepaling verder in overeenstemming te brengen met artikel 46*quater* Sv.

Via de programmawet van 1 juli 2016 (*BS* 4 juli 2016) verkreeg het Openbaar Ministerie een wettelijk toegangsrecht tot het Centraal Aanspreekpunt gehouden door de Nationale Bank van België (CAP), initieel ingesteld via artikel 322, § 3, eerste lid van het Wetboek van de inkomstenbelastingen 1992, om de in artikel 46*quater*, § 1, eerste lid Sv bedoelde informatie te bekomen. Ook de inlichtingen- en veiligheidsdiensten hebben elk op zich een toegangsrecht, *op grond van een gecombineerde lezing van artikel 14, 2de lid en van artikel 18/15 WIV. De modaliteiten van dit toegangsrecht werden* vastgelegd

étaient définis dans un protocole d'accord entre la Banque nationale de Belgique et le service de renseignement et de sécurité concerné:

— Convention du 24 août 2020 relative à l'accès de la Sûreté de l'État au point de contact central de la Banque nationale de Belgique, signé par le gouverneur de la Banque nationale de Belgique et l'administrateur général de la Sûreté de l'État.

— Convention du 14 juin 2016 relative à l'accès du Service général du Renseignement et de la Sécurité au point de contact central de la Banque nationale de Belgique, signé par la gouverneur Banque nationale de Belgique et le chef du Service général du Renseignement et de la Sécurité.

Pour des raisons de sécurité juridique, la décision a été prise de convertir ce droit d'accès implicite des services de renseignement et de sécurité en un droit d'accès explicite, comme c'est le cas pour le ministère public.

Une correction dans la version française été apportée pour rendre le § 3, alinéa 1er conforme à la version néerlandophone.

Enfin, l'article 46*quater*, § 2, a), du Code d'instruction criminelle donne la possibilité au ministère public d'être informé en temps réel des différentes opérations effectuées sur un compte bancaire ou en rapport avec un coffre bancaire. Cette disposition prévoit que: "*Lorsque les nécessités de l'information le requièrent, le procureur du Roi peut en outre requérir que […] pendant une période renouvelable d'au maximum deux mois, les transactions bancaires afférentes à un ou plusieurs de ces comptes bancaires, ou de ces coffres bancaires ou instruments financiers du suspect, seront observées*". Cette faculté de collecter des données en temps réel est comparable à la compétence d'enquête pénale visée à l'article 88*bis* du Code d'instruction criminelle, qui prévoit la possibilité de collecter des données en temps réel dans le secteur des télécommunications.

Bien que les services de renseignement et de sécurité disposent d'une même possibilité de collecter des données en temps réel dans le secteur des télécommunications (par le biais de l'article 18/8 de la LRS, une disposition similaire à l'article 88*bis* du Code d'instruction criminelle), il n'existe actuellement pas de moyen légal analogue pour le secteur financier. Or le placement immédiat sous surveillance d'une personne visée dans le cadre des missions de renseignement de la Sûreté de l'État et du Service Général du Renseignement et de la Sécurité présente clairement une valeur ajoutée, notamment dans le domaine de la lutte contre le terrorisme,

in een protocolakkoord tussen de Nationale Bank van België en de betrokken inlichtingen- en veiligheidsdienst:

— Overeenkomst van 24 augustus 2020 inzake de toegang van de Veiligheid van de Staat tot het Centraal Aanspreekpunt van de Nationale Bank van België, ondertekend door de gouverneur van de Nationale Bank van België en de administrateur-generaal van de Veiligheid van de Staat.

— Overeenkomst van 14 juni 2016 inzake de toegang van de Algemene Dienst Inlichting en Veiligheid tot het Centraal Aanspreekpunt van de Nationale Bank van België, ondertekend door de gouverneur van de Nationale Bank van België en de chef van de Algemene Dienst Inlichting en Veiligheid.

Er wordt om redenen van rechtszekerheid geopteerd om dit impliciet toegangsrecht van de inlichtingen- en veiligheidsdiensten, net zoals bij het Openbaar Ministerie, om te zetten in een expliciet toegangsrecht.

Een correctie in de Franstalige versie werd doorgevoerd om § 3, eerste lid in overeenstemming te brengen met de Nederlandstalige versie.

Artikel 46*quater*, § 2, a) Sv tenslotte geeft het Openbaar Ministerie de mogelijkheid om in 'real time' op de hoogte te worden gehouden van de verschillende verrichtingen die op een bankrekening of met betrekking tot een bankkluis plaatsgrijpen. Deze bepaling stelt: *"Ingeval de noodwendigheden van het opsporingsonderzoek dit vergen, kan de procureur des Konings bovendien vorderen dat […] gedurende een vernieuwbare periode van maximum twee maanden de bankverrichtingen met betrekking tot een of meerdere van deze bankrekeningen, bankkluizen of financiële instrumenten van de verdachte onder toezicht worden geplaatst"*. Deze bevoegdheid om in 'real time' gegevens in te winnen is vergelijkbaar met de strafrechtelijke onderzoeksbevoegdheid in artikel 88*bis* Sv waar een wettelijke mogelijkheid is voorzien om 'real time' gegevens in te winnen bij de telecomsector.

Hoewel de inlichtingen- en veiligheidsdiensten eenzelfde mogelijkheid hebben om 'real time' gegevens in te winnen bij de telecomsector (via artikel 18/8 WIV, een bepaling vergelijkbaar met artikel 88*bis* Sv), bestaat actueel geen eenzelfde wettelijk middel ten aanzien van de financiële sector. Nochtans heeft het rechtstreeks onder toezicht plaatsen van een geviseerd persoon binnen de inlichtingenopdrachten van de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid een duidelijke meerwaarde, niet in het minst binnen het bestrijden van het terrorisme, waaronder de financiering van terrorisme, de spionage en de criminele organisaties.

dont le financement du terrorisme, de l'espionnage et des organisations criminelles. La présente modification de loi octroie cet instrument légal aux deux services de renseignement et de sécurité. L'option a clairement été retenue d'intégrer cette nouvelle méthode de renseignement dans la catégorie des méthodes exceptionnelles, ce qui a pour effet que leur mise en œuvre est soumise au régime le plus strict en termes de conditions d'application, de procédure et de mécanismes de contrôle externe.

L'obligation de collaboration (cf. article 18/15 de la LRS) et l'obligation de secret y relative (cf. article 36 de la LRS) s'étendent à chaque institution financière et à chaque personne qui offre ou propose une opération, un produit ou un service de nature financière, quelle qu'en soit la forme, sur le territoire belge. A cet égard, il est renvoyé à la description mentionnée au paragraphe 1er.

Conformément à l'article 46*quater* du Code d'instruction criminelle, afin de garantir que les données soient fournies numériquement et sous une forme qui permette une exploitation aisée, il est également repris que la communication d'informations par les personnes et institutions doit avoir lieu sous forme numérique, de la manière établie par le service de renseignement et de sécurité concerné. L'exigence relative à la présentation de la carte de légitimation, un acte qui n'est pas effectué dans la pratique compte tenu des procédures de demandes par voie numérique, est dès lors supprimée.

Conformément à l'article 16/6, la coopération du PCC s'effectue également en prenant en compte des dispositions spécifiques inscrites dans la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt.

L'article 18/15 de la LRS prévoit que l'institution requise est tenue de remettre les informations demandées sans délai.

Les peines liées au non-respect de l'obligation de collaboration, modifiées par la loi du 30 mars 2017, ou les peines réprimant la violation de l'obligation de secret demeurent inchangées.

Art. 27

À l'article 20, à la demande du Comité R, le mot "collaboration" est remplacé par le mot "coopération" dans la version française du texte.

Voorliggende wetwijziging kent dit wettelijke instrument aan beide inlichtingen- en veiligheidsdiensten toe. Er wordt duidelijk geopteerd om deze nieuwe inlichtingenmethode onder te brengen binnen de categorie van uitzonderlijke methoden, wat met zich meebrengt dat de aanwending ervan onderhevig is aan het meest strenge regime inzake toepassingsvoorwaarden, procedure en externe controlemechanismen.

De medewerkingsplicht (*cf.* artikel 18/15 WIV) en daarmee gepaard gaande geheimhoudingsplicht (*cf.* artikel 36 WIV) strekt zich uit tot de elke financiële instelling en elke persoon die een verrichting, product of dienst van financiële aard, ongeacht de verschijningvorm, beschikbaar stelt of aanbiedt binnen het Belgische grondgebied. Hiermee wordt verwezen naar de omschrijving in de eerste paragraaf.

Net zoals voorzien in artikel 46*quater* Sv wordt er, teneinde te verzekeren dat de gegevens digitaal worden aangeleverd en onder een vorm die op eenvoudige wijze een exploitatie toelaat, tevens opgenomen dat de mededeling van informatie door de personen en instellingen moet gebeuren in een digitale vorm, in de wijze die bepaald wordt door de betrokken inlichtingen- en veiligheidsdienst. De vereiste van het vertonen van legitimatiekaart, een handeling die in de praktijk niet voorkomt gelet op de digitale aanvraagprocedures, wordt om die redenen ook geschrapt.

Net zoals in artikel 16/6 gebeurt de medewerking van het CAP eveneens rekening houdend met de specifieke bepalingen die zijn ingeschreven in de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van bankrekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest.

Artikel 18/15 WIV voorziet dat de gevorderde instelling ertoe gehouden is de gevraagde informatie onverwijld te verstrekken.

De straffen waarmee het niet voldoen aan de medewerkingsplicht, zoals gewijzigd met de wet van 30 maart 2017, of de straffen waarmee het schenden van de geheimhoudingsplicht worden bestraft, worden niet gewijzigd.

Art. 27

In artikel 20 wordt op vraag van het Comité I het woord *"collaboration"* vervangen door het woord *"coopération"* in de Franse versie van de tekst.

Comme suggéré au point 75 de l'avis du Comité R, les mots "dans les limites d'un protocole approuvé par les ministres concernés "sont supprimés et la phrase est scindée en deux pour une meilleure compréhension.

En outre, en réponse au point 75 du Comité R, les auteurs ne voient pas la plus-value de définir la notion d'assistance technique dans le présent texte étant donné qu'une circulaire confidentielle existe entre les services de renseignement et le pouvoir judiciaire afin d'en délimiter les contours.

Ainsi, si une administration publique a besoin d'une assistance technique d'urgence, par exemple en matière Cyber, il convient d'éviter que l'assistance technique ponctuelle doive être refusée dans l'attente de la signature d'un protocole.

Le ministre de la Justice,

Vincent VAN QUICKENBORNE

La ministre de la Défense,

Ludivine DEDONDER

Zoals voorgesteld in punt 75 van het advies van het Comité I worden de woorden "binnen de perken van een protocol goedgekeurd door de betrokken ministers" weggelaten en wordt de zin, voor een beter begrip, gedeeld in twee zinnen.

Overigens, als antwoord op punt 75 van het Comité I, zien de auteurs geen meerwaarde in het definiëren van het begrip technische bijstand in de huidige tekst, rekening houdend met het feit dat een bestaande vertrouwelijke omzendbrief tussen de inlichtingendiensten en de rechterlijke macht de contouren ervan afbakent.

Indien een overheidsdienst dringend technische bijstand nodig heeft, bijvoorbeeld in cyberaangelegenheden, moet worden vermeden dat ad hoc technische bijstand wordt geweigerd in afwachting van de ondertekening van een protocol.

De minister van Justitie,

Vincent VAN QUICKENBORNE

De minister van Defensie,

Ludivine DEDONDER

AVANT-PROJET DE LOI

soumis à l'avis du Conseil d'État

Avant-projet de loi modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

Article 1er

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

Art. 2

Art. 2. À l'article 3 de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, modifiée par les lois du 6 décembre 2015, 29 janvier 2016 et 21 avril 2016, les modifications suivantes sont apportées:

1° dans la disposition 6° le mot "commission" est remplacé par le mot "Commission";

2° une disposition 8°/1 est insérée, rédigée comme suit:

"8°/1 "son délégué": l'agent, autre que le gestionnaire du dossier, désigné par le dirigeant du service pour prendre habituellement certaines décisions à sa place;";

3° dans la disposition 9°, b) les mots "revêtu au moins du grade de commissaire" sont remplacés par les mots "de niveau A désigné pour effectuer certaines missions spécifiques prévues dans la présente loi".

Art. 3

À l'article 11 de la même loi, les modifications suivantes sont apportées:

1° dans la version néerlandaise, au paragraphe 1er 2°, le mot "beheerst" est remplacé par le mot "beheert" et les mots "des conflits armés" sont remplacés par le mot "international";

2° au paragraphe 1er, est inséré un 2°/1 rédigé comme suit:

"2°/1 de neutraliser, dans le cadre d'une crise nationale de cybersécurité, une cyberattaque de systèmes informatiques et de communications non gérés par la Défense et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit international;"

VOORONTWERP VAN WET

onderworpen aan het advies van de Raad van State

Voorontwerp van wet tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten

Artikel 1

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

Art. 2

Art. 2. In artikel 3 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, gewijzigd bij de wetten van 6 december 2015, 29 januari 2016 en 21 april 2016, worden de volgende wijzigingen aangebracht:

1° in de bepaling onder 6° wordt het woord "commissie" vervangen door het woord "Commissie";

2° er wordt een bepaling onder 8°/1 ingevoegd, luidende:

"8°/1 "zijn gedelegeerde": de agent, andere dan de dossierbeheerder, aangesteld door het diensthoofd om bepaalde beslissingen gewoonlijk in zijn plaats te nemen;";

3° in de bepaling onder 9°, b) worden de woorden "die ten minste de graad van commissaris heeft" vervangen door de woorden "van niveau A die belast is met specifieke bepaalde opdrachten voorzien in deze wet ";

Art. 3

In artikel 11 van dezelfde wet, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, 2°, wordt het woord "beheerst" vervangen door het woord "beheert" en worden de woorden "recht van de gewapende conflicten" vervangen door de woorden "internationaal recht".
2° in paragraaf 1, wordt onder 2°/1 een bepaling ingevoegd, luidende:

"2°/1 het neutraliseren, in het kader van een nationale cyber security crisis, van een cyberaanval op informatica- en verbindingssystemen niet beheerd door de Minister van Landsverdediging en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het internationaal recht;"

3° au paragraphe 1er, est inséré un 6° rédigé comme suit:

"6° d'exécuter toutes autres missions qui lui sont confiées par ou en vertu de la loi;"

4° au paragraphe 2, est inséré un 5° rédigé comme suit:

"5° "crise nationale de cybersécurité": tout incident de cybersécurité qui, par sa nature ou ses conséquences:
- menace les intérêts vitaux du pays ou les besoins essentiels de la population;
- requiert des décisions urgentes;
- et demande une action coordonnée de plusieurs départements et organismes;

5° au paragraphe 3, alinéa 1 les mots "paragraphe 1er, 1°, 2°, 3° et 5°" sont remplacés par les mots "paragraphe 1er, 1° à 3°, 5° et 6°".

Art. 4

Dans le Chapitre III, la Section 2, il est inséré une sous-section 1, rédigée comme suit: "Sous-section 1. Exemptions de peine"

Art. 5

Dans la sous-section 1, insérée par l'article 4, à l'article 13/1, inséré par la loi du 4 février 2010 et modifié par la loi du 30 mars 2017, les modifications suivantes sont apportées:

1° l'actuel alinéa 1er formera le paragraphe 1er;

2° à l'alinéa 2, qui formera le paragraphe 2, les mots "à l'alinéa" sont remplacés par les mots "au paragraphe 1er"; dans la version néerlandaise, le mot "begaan" est remplacé par le mot "plegen"; dans la version néerlandaise, les mots "van de uitvoering" sont abrogés; les mots "la méthode" sont remplacés par les mots "leur mission" et les mots "d'autres personnes" sont remplacés par les mots "de tiers";

3° les alinéas 3, 4, 5 et 6 sont abrogés et remplacés par les paragraphes 3, 4, 5, 6, 7, 8, et 9, rédigés comme suit:

"§3. Sans préjudice du paragraphe 2, sont exemptés de peine, les agents qui, lors de l'exécution des missions visées aux articles 7, 1° et 3°/1 et 11, §1er, 1° à 3° et 5°, commettent des infractions absolument nécessaires afin d'assurer l'exécution optimale de leur mission ou de garantir leur propre sécurité ou celle de tiers.

3° in paragraaf 1, wordt onder 6° een bepaling ingevoegd, luidende:

"6° het uitvoeren van alle opdrachten die hem door of krachtens de wet worden toevertrouwd."

4° in paragraaf 2, wordt onder 5° een bepaling ingevoegd, luidende

"5° "nationale cyber security crisis": elke cyber security gebeurtenis die wegens haar aard of gevolgen:
- de vitale belangen van het land of de essentiële behoeften van de bevolking bedreigt;
- een dringende besluitvorming vereist;
- en de gecoördineerde inzet van verscheidene departementen en organismen vergt."

5° in paragraaf 3, eerste lid worden de woorden "paragraaf 1, 1°, 2°, 3° en 5°" vervangen door de woorden "paragraaf 1, 1° tot 3°, 5° en 6°".

Art. 4

In Hoofdstuk III, Afdeling 2, wordt een onderafdeling 1 ingevoegd, luidende: "Onderafdeling 1. Strafuitsluitingsgronden"

Art. 5

In onderafdeling 1, ingevoegd bij artikel 4, worden in artikel 13/1, ingevoegd door de wet van 4 februari 2010 en gewijzigd bij de wet van 30 maart 2017, volgende wijzigingen aangebracht:

1° de bestaande tekst van het eerste lid zal paragraaf 1 vormen;

2° in het huidige tweede lid, waarvan de bestaande tekst paragraaf 2 zal vormen, worden de woorden "het eerste lid" vervangen door de woorden "paragraaf 1"; het woord "begaan" vervangen door het woord "plegen"; de woorden "van de uitvoering" opgeheven; de woorden "de methode" vervangen door de woorden "hun opdracht" en de woorden "andere personen" vervangen door het woord "derden";

3° de leden 3, 4, 5 en 6 worden opgeheven en vervangen door de paragrafen 3, 4, 5, 6, 7, 8 en 9, luidende:

"§3. Onverminderd paragraaf 2, blijven vrij van straf, de agenten die in de uitvoering van de opdrachten bedoeld in de artikelen 7, 1° en 3°/1 en 11, §1, 1° tot 3° en 5°, strafbare feiten plegen die strikt noodzakelijk zijn voor het welslagen van hun opdracht of ter verzekering van hun eigen veiligheid of die van derden.

Les infractions visées à l'alinéa 1er ne peuvent être commises qu'avec l'accord écrit préalable de la Commission. La Commission donne son accord dans les quatre jours suivant la réception de la demande écrite et motivée du dirigeant du service.

L'accord ne peut porter sur une période supérieure à six mois, sans préjudice de la possibilité de prolonger la mesure en suivant la procédure visée à l'alinéa 2.

La demande du dirigeant du service mentionne, sous peine d'illégalité:
1° les faits susceptibles d'être qualifiés infraction(s);
2° le contexte de la demande et la finalité;
3° l'absolue nécessité;
4° la proportionnalité visée au paragraphe 7;
5° la période durant laquelle la ou les infractions peuvent être commises et la motivation de la durée de la période;
6° le cas échéant, les motifs qui justifient l'extrême urgence visée au paragraphe 5;
7° la date de la demande;
8° la signature du dirigeant du service.

§4. L'agent fait rapport par écrit au dirigeant du service le plus rapidement possible après la commission de l'infraction. Le dirigeant du service en informe la Commission par écrit sans délai.

Par dérogation à l'alinéa 1er, si la mesure a été autorisée pour une période supérieure à deux mois, le service de renseignement et de sécurité concerné informe tous les mois par écrit la Commission du déroulement de la mesure.

§5. En cas d'extrême urgence, le dirigeant du service demande l'accord verbal préalable du président de la Commission ou, en cas d'indisponibilité, d'un autre membre. L'auteur de l'accord en informe immédiatement les autres membres. Le dirigeant du service confirme sa demande par écrit dans les vingt-quatre heures suivant la communication de l'accord. La Commission confirme également son accord par écrit le plus rapidement possible. Cet accord est valable cinq jours.

§6. Si, en raison de circonstances imprévisibles, une infraction a été commise pour laquelle la procédure prévue aux paragraphes 3 ou 5 n'a pas pu être suivie, le dirigeant du service en informe la Commission dans les plus brefs délais. L'agent bénéficie de l'exemption de peine si la Commission estime que l'infraction était imprévisible et strictement nécessaire pour assurer sa propre sécurité ou celle de tiers**.**

De strafbare feiten, bedoeld in het eerste lid, kunnen slechts worden gepleegd na voorafgaand schriftelijk akkoord van de Commissie. De Commissie geeft haar akkoord binnen de vier dagen na ontvangst van de schriftelijke en gemotiveerde vraag van het diensthoofd.

Het akkoord geldt voor een maximumtermijn van zes maanden, onverminderd de mogelijkheid om de maatregel te verlengen volgens de procedure bedoeld in het tweede lid.

De vraag van het diensthoofd vermeldt, op straffe van onwettigheid:
1° de feiten die als misdrijf kunnen worden gekwalificeerd;
2° de context van de vraag en de finaliteit;
3° de strikte noodzakelijkheid;
4° de proportionaliteit bedoeld in paragraaf 7;
5° de periode waarbinnen de strafbare feiten kunnen worden gepleegd en de motivering van de duur van deze periode;
6° in voorkomend geval, de redenen die de hoogdringendheid bedoeld in paragraaf 5 rechtvaardigen;
7° de datum van de vraag;
8° de handtekening van het diensthoofd.

§4. De agent brengt zo spoedig mogelijk na het plegen van het strafbaar feit schriftelijk verslag uit aan het diensthoofd. Het diensthoofd informeert onverwijld schriftelijk de Commissie.

In afwijking van het eerste lid, indien de maatregel is toegestaan voor een periode langer dan twee maanden, brengt de betrokken inlichtingen- en veiligheidsdienst maandelijks schriftelijk verslag uit aan de Commissie over het verloop van de maatregel.

§5. In geval van hoogdringendheid vraagt het diensthoofd vooraf het mondeling akkoord van de voorzitter van de Commissie of, bij onbereikbaarheid, van een ander lid. Diegene die het akkoord gegeven heeft, brengt de overige leden/magistraten hiervan onmiddellijk op de hoogte. Het diensthoofd bevestigt zijn vraag schriftelijk binnen de vierentwintig uur na mededeling van het akkoord. De Commissie bevestigt eveneens zo spoedig mogelijk schriftelijk haar akkoord. Dit akkoord geldt voor vijf dagen.

§6. Indien door onvoorziene omstandigheden een strafbaar feit gepleegd is waarbij de procedure bedoeld in de paragrafen 3 of 5 niet gevolgd kon worden, brengt het diensthoofd dit zo spoedig mogelijk ter kennis van de Commissie. De agent blijft vrij van straf indien de Commissie oordeelt dat het strafbaar feit niet voorzienbaar was en strikt noodzakelijk was ter verzekering van de eigen veiligheid of van derden.

Art. 6

Dans le Chapitre III, Section 2, Sous-section 1, insérée par l'article 6, il est inséré un article 13/1/1, rédigé comme suit:

"Art. 13/1/1. §1. Il est interdit aux sources humaines de commettre des infractions.

§2. Par dérogation au paragraphe 1, sont exemptés de peine les sources humaines majeures d'âge inscrites dans le registre des sources humaines du service de renseignement et de sécurité concerné qui commettent des infractions absolument nécessaires afin d'assurer leur position d'information ou de garantir leur propre sécurité ou celle de tiers.

Les infractions ne peuvent être commises qu'avec l'accord écrit préalable de la Commission. La Commission donne son accord dans les quatre jours suivant la réception de la demande écrite et motivée du dirigeant du service.

L'accord ne peut porter sur une période supérieure à deux mois, sans préjudice de la possibilité de prolonger la mesure en suivant la procédure visée à l'alinéa 2.

La demande du dirigeant du service mentionne, sous peine d'illégalité:
1° le code d'identification de la source humaine;
2° les faits susceptibles d'être qualifiés infraction(s);
3° le contexte de la demande et la finalité;
4° la synthèse de l'analyse de risque(s) sur les faits susceptibles d'être qualifiés infraction(s);
5° l'absolue nécessité;
6° la proportionnalité visée au paragraphe 6;
7° les conditions strictes imposées à la source humaine;
8° la période durant laquelle la ou les infractions peuvent être commises et la motivation de la durée de la période;
9° le cas échéant, les motifs qui justifient l'extrême urgence visée au paragraphe 5;
10° la date de la demande;
11° la signature du dirigeant du service.

§3. Avant que l'infraction autorisée ne puisse être commise, la source humaine signe un mémorandum contenant notamment les modalités de mise en œuvre et de rapportage. Ce mémorandum est conservé dans le dossier individuel de la source humaine.

§4. Dès que l'infraction a été commise et que la source humaine est en sécurité pour le faire, celle-ci fait rapport à son officier traitant. Ce dernier en informe par écrit le dirigeant du service qui, à son tour, informe par écrit la Commission dans les meilleurs délais.

Art. 6

In Hoofdstuk III, Afdeling 2, Onderafdeling 1, ingevoegd bij artikel 6, wordt een artikel 13/1/1 ingevoegd, luidende:

"Art. 13/1/1. §1. Het is de menselijke bronnen verboden strafbare feiten te plegen.

§2. In afwijking van paragraaf 1, blijven vrij van straf, de meerderjarige menselijke bronnen die ingeschreven zijn in het register van menselijke bronnen van de betrokken inlichtingen- en veiligheidsdienst die strafbare feiten plegen die strikt noodzakelijk zijn ter verzekering van hun informatiepositie of ter verzekering van hun eigen veiligheid of die van derden.

De strafbare feiten kunnen slechts worden gepleegd na voorafgaand schriftelijk akkoord van de Commissie. De Commissie geeft haar akkoord binnen de vier dagen na ontvangst van de schriftelijke en gemotiveerde vraag van het diensthoofd.

Het akkoord geldt voor een maximumtermijn van twee maanden, onverminderd de mogelijkheid om de maatregel te verlengen volgens de procedure bedoeld in het tweede lid.

De vraag van het diensthoofd vermeldt, op straffe van onwettigheid:
1° de identificatiecode van de menselijke bron; 2° de feiten die als misdrijf kunnen worden gekwalificeerd;
3° de context van de vraag en de finaliteit;
4° de synthese van de risicoanalyse over de beoogde feiten die als misdrijf kunnen worden gekwalificeerd;
5° de strikte noodzakelijkheid;
6° de proportionaliteit bedoeld in paragraaf 6;
7° de strikte voorwaarden opgelegd aan de menselijke bron;
8° de periode tijdens dewelke strafbare feiten begaan kunnen worden en de motivering van de duur van deze periode;
9° in voorkomend geval, de redenen die de hoogdringendheid bedoeld in paragraaf 5 rechtvaardigen;
10° de datum van de vraag;
11° de handtekening van het diensthoofd.

§3. Vooraleer het toegelaten strafbaar feit kan worden gepleegd, ondertekent de menselijke bron een memorandum dat onder meer de modaliteiten voor de tenuitvoerlegging en de verslaggeving bevat. Dit memorandum wordt bewaard in het individueel dossier van de menselijke bron.

§4. Zodra het strafbaar feit gepleegd is en de menselijke bron in veiligheid is, brengt deze verslag uit aan zijn behandelende officier. Deze laatste informeert schriftelijk het diensthoofd dat, op zijn beurt, zo spoedig mogelijk de

Art. 7

Dans le Chapitre III, Section 2, Sous-section 1, insérée par l'article 6, il est inséré un article 13/1/2, rédigé comme suit:

"Art. 13/1/2. §1. Lors de l'application des articles 13/1 et 13/1/1, la Commission fonctionne selon les modalités déterminées à l'article 43/1.

§2. Sont exemptés de peine, les membres de la Commission qui autorisent la commission des infractions visées aux articles 13/1 et 13/1/1.

§3. Sont exemptés de peine, les membres et les collaborateurs du Comité permanent R, lorsqu'ils exercent leur contrôle dans le cadre de l'application de la présente sous-section.

§4. Sont exemptés de peine, le dirigeant du service et les membres des services de renseignement et de sécurité qui encadrent ou contrôlent les agents visés à l'article 13/1 et les sources humaines visées à l'article 13/1/1."

Art. 7

In Hoofdstuk III, Afdeling 2, Onderafdeling 1, ingevoegd bij artikel 6, wordt een artikel 13/1/2 ingevoegd, luidende:

"Art. 13/1/2. §1. In de toepassing van de artikelen 13/1 en 13/1/1, treedt de Commissie op volgens de modaliteiten bepaald in artikel 43/1.

§2. Blijven vrij van straf, de leden van de Commissie die een akkoord verlenen tot het plegen van strafbare feiten zoals bedoeld in de artikelen 13/1 en 13/1/1.

§3. Blijven vrij van straf, de raadsleden en de medewerkers van het Vast Comité I wanneer zij hun toezicht uitoefenen binnen de toepassing van deze onderafdeling.

§4. Blijven vrij van straf, het diensthoofd en de leden van de inlichtingen- en veiligheidsdiensten die de agenten bedoeld in artikel 13/1 en de menselijke bronnen bedoeld in artikel 13/1/1, begeleiden of controleren."

Art. 8

Dans le Chapitre III, Section 2, il est inséré une sous-section 2, rédigée comme suit:
"Sous-section 2. Faux nom, identité et qualité fictives"

Art. 8

In Hoofdstuk III, Afdeling 2, wordt na artikel 13/1/2 een onderafdeling 2 ingevoegd, luidende: "Onderafdeling 2. Valse naam, fictieve identiteit en hoedanigheid"

Art. 9

À l'article 13/2, inséré par la loi 30 mars 2017, les modifications suivantes sont apportées:

1° le texte actuel des alinéas 1 à 6 formera le paragraphe 1er;

2° l'alinéa 2 est abrogé;

3° l'alinéa 3 devient l'alinéa 2 du paragraphe 1er et les mots "temporaire et" sont abrogés;

3° il est inséré un paragraphe 2, rédigé comme suit:

"§2. Sans préjudice du §1er, l'utilisation d'une identité fictive pour protéger l'agent lorsqu'il collecte des données dans le cadre d'une méthode requiert l'accord écrit préalable de la Commission. Celle-ci donne son accord dans les quatre jours suivant la réception de la demande écrite et motivée du dirigeant du service.

L'accord ne peut porter sur une période supérieure à six mois, sans préjudice de la possibilité de prolonger la mesure en suivant la procédure visée à l'alinéa 1er.

Art. 9

In artikel 13/2, ingevoegd bij de wet van 30 maart 2017, worden de volgende wijzigingen aangebracht:

1° de bestaande tekst van het eerste tot en met zesde lid vormen paragraaf 1;

2° het tweede lid is opgeheven;

3° in het derde lid, dat paragraaf 1, derde lid is geworden, worden de woorden "tijdelijk en" opgeheven;

3° er wordt een paragraaf 2 ingevoegd, luidende:

"§2. Onverminderd §1, vereist het gebruik van een fictieve identiteit ter bescherming van de agent tijdens het verzamelen van gegevens in het kader van een methode het voorafgaandelijk schriftelijk akkoord van de Commissie. Deze geeft haar akkoord binnen de vier dagen na ontvangst van de schriftelijke en gemotiveerde vraag van het diensthoofd.

Het akkoord geldt voor een maximumtermijn van zes maanden, onverminderd de mogelijkheid om de maatregel te verlengen volgens de procedure bedoeld in het eerste lid.

La demande du dirigeant du service mentionne, sous peine d'illégalité:

1° la(es) méthode(s) en appui de laquelle/desquelles l'identité fictive peut être utilisée;
2° les raisons de sécurité liées à la protection de l'agent ou de tiers;
3° la période durant laquelle l'identité fictive peut être utilisée et la motivation de la durée de la période;
4° le cas échéant, les motifs qui justifient l'extrême urgence visée à l'alinéa 4;
5° la date de la demande;
6° la signature du dirigeant du service.

En cas d'extrême urgence, le dirigeant du service demande l'accord verbal préalable du président de la Commission ou, en cas d'indisponibilité, d'un autre membre. L'auteur de l'accord en informe immédiatement les autres membres. Le dirigeant du service confirme sa demande par écrit dans les vingt-quatre heures suivant la communication de l'accord. La Commission confirme également son accord par écrit le plus rapidement possible. Cet accord est valable cinq jours.

La Commission transmet sans délai tous les documents visés dans le présent paragraphe au Comité permanent R.

L'agent fait rapport par écrit au dirigeant du service, ou à l'agent qu'il désigne à cet effet, tous les quinze jours sur le déroulement de la mesure. Le service de renseignement et de sécurité concerné informe tous les quinze jours par écrit la Commission du déroulement de la mesure.

Le dirigeant du service met fin à la mesure lorsque les raisons de sécurité liées à la protection de l'agent ou de tiers ont disparu ou lorsqu'il a été constaté une illégalité. Il en informe dès que possible la Commission.

Lorsque la Commission ou le Comité permanent R constate une illégalité, il est mis fin à la mesure en cours ou planifiée dès que possible pour ne pas mettre la méthode de recueil de données en péril et en tenant compte des risques encourus par l'agent.

Lors de l'application du présent paragraphe, la Commission fonctionne selon les modalités déterminées à l'article 43/1."

Art. 10

Dans le Chapitre III, Section 2, il est inséré une sous-section 3, rédigée comme suit: "Sous-section 3. La création et l'utilisation d'une personne morale"

Art. 11

Dans le Chapitre III, Section 2, il est inséré une sous-section 4, rédigée comme suit: "Sous-section 4. Le concours de tiers".

De vraag van het diensthoofd vermeldt op straffe van onwettigheid:

1° de methode ter ondersteuning waarvan de fictieve identiteit kan worden gebruikt;
2° de veiligheidsredenen verbonden aan de bescherming van de agent of derden;
3° de periode waarbinnen de fictieve identiteit kan worden aangewend en de motivering van de duur van deze periode;
4° in voorkomend geval, de redenen die de hoogdringendheid bedoeld in het vierde lid rechtvaardigen;
5° de datum van de vraag;
6° de handtekening van het diensthoofd.

In geval van hoogdringendheid, vraagt het diensthoofd vooraf het mondeling akkoord van de voorzitter van de Commissie of, bij onbereikbaarheid, van een ander lid. Diegene die het akkoord gegeven heeft, brengt de overige leden hiervan onmiddellijk op de hoogte. Het diensthoofd bevestigt zijn vraag schriftelijk binnen de vierentwintig uur na de mededeling van het akkoord. De Commissie bevestigt eveneens zo spoedig mogelijk schriftelijk haar akkoord. Dit akkoord geldt voor vijf dagen.

De Commissie maakt alle documenten bedoeld in de deze paragraaf onverwijld over aan het Vast Comité I.

De agent brengt om de 15 dagen schriftelijk verslag uit over de voortgang van de maatregel aan het diensthoofd of de agent die hij daartoe aanstelt. De betrokken inlichtingen- en veiligheidsdienst stelt de Commissie om de 15 dagen schriftelijk op de hoogte van het verloop van de maatregel.

Het diensthoofd beëindigt de maatregel wanneer de veiligheidsmaatregelen verbonden aan de bescherming van de agent of derden zijn weggevallen of wanneer hij een onwettigheid heeft vastgesteld. Hij brengt zijn beslissing zo spoedig mogelijk ter kennis van de Commissie.
Indien de Commissie of het Vast Comité I een onwettigheid vaststelt, wordt de geplande of lopende maatregel zo snel mogelijk beëindigd en rekening houdend met de risico's die zulks meebrengt voor de agent.

In de toepassing van deze paragraaf, treedt de Commissie op volgens de modaliteiten bepaald in artikel 43/1."

Art. 10

In Hoofdstuk III, Afdeling 2, wordt na artikel 13/2 een onderafdeling 3 ingevoegd, luidende: "Onderafdeling 3. De oprichting en inzet van rechtspersonen"

Art. 11

In Hoofdstuk III, Afdeling 2, wordt na artikel 13/3 een onderafdeling 4 ingevoegd, luidende: "Onderafdeling 4. De medewerking van derden".

Art. 12

À l'article 13/4 de la même loi, inséré par la loi du 30 mars 2017, les modifications suivantes sont apportées:

1° à l'alinéa 3, les mots "alinéas 2, 3 et 5" sont remplacés par les mots "paragraphes 2 à 5 et 7 à 9"; les mots "et le §9 de l'article 13/1/1" sont insérés entre les mots "de l'article 13/1" et les mots "sont applicables aux tiers"; les mots "ont fourni" sont remplacés par le mot "fournissent";

2° l'article est complété par un alinéa rédigé comme suit:

"L'aide et l'assistance apportées se font toujours sous le contrôle du service de renseignement et de sécurité concerné, qui garde la direction de l'opération.".

Art. 12

In artikel 13/4 van dezelfde wet, ingevoegd bij de wet van 30 maart 2017, worden de volgende wijzigingen aangebracht:

1° in het derde lid worden de woorden "Het tweede, derde en vijfde lid" vervangen door de woorden "De paragrafen 2 tot 5 en 7 tot 9"; de woorden "en paragraaf 9 van artikel 13/1/1" worden ingevoegd tussen de woorden "van artikel 13/1" en de woorden "zijn van toepassing op de derden"; de woorden "hebben verleend" worden vervangen door het woord "verlenen";

2° het artikel wordt aangevuld met een lid, luidende:

"De verleende hulp en bijstand geschiedt te allen tijde onder het toezicht van de betrokken inlichtingen- en veiligheidsdienst die de leiding behoudt over de operatie.".

Art. 13

À l'article 16/3 de la même loi, inséré par la loi du 25 décembre 2016, les modifications suivantes sont apportées:

1° au paragraphe 2, alinéa 1er, les mots "ou son délégué" sont insérés entre les mots "le dirigeant du service" et les mots "et communiquée";

2° au paragraphe 2, un alinéa rédigé comme suit est inséré entre les alinéas 1 et 2:

"En cas d'urgence, le dirigeant du service ou son délégué peut décider d'accéder à ces données verbalement. Cette décision verbale est confirmée dans un délai de vingt-quatre heures par une décision écrite, selon les modalités fixées à l'alinéa 1er.";

3° au paragraphe 2, alinéa 2, devenu alinéa 3, les mots "les conditions" sont remplacés par les mots "des circonstances".

Art. 13

In artikel 16/3 van dezelfde wet, ingevoegd bij de wet van 25 december 2016, worden de volgende wijzigingen aangebracht:

1° in paragraaf 2, eerste lid, worden de woorden "een diensthoofd" vervangen door de woorden "het diensthoofd of zijn gedelegeerde";

2° in paragraaf 2 wordt tussen het eerste en het tweede lid een lid ingevoegd, luidende:

"In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde mondeling beslissen om toegang te hebben tot deze gegevens. Deze mondelinge beslissing wordt binnen vierentwintig uur bevestigd door een schriftelijke beslissing, volgens de nadere regels bepaald in het eerste lid.";

3° in paragraaf 2, tweede lid, dat het derde lid is geworden, worden de woorden "les conditions" in de Franse tekst vervangen door de woorden "des circonstances".

Art. 14

À l'article 16/4, § 2, de la même loi, inséré par la loi du 21 mars 2018, les modifications suivantes sont apportées:

1° au paragraphe 2, 1er alinéa , le mot"artikels" est remplacé par le mot "artikelen" dans la version néerlandaise;

Art. 14

In artikel 16/4 van dezelfde wet, ingevoegd bij de wet van 21 maart 2018, worden de volgende wijzigingen aangebracht:

1° in paragraaf 2, eerste lid wordt het woord "artikels" vervangen door het woord "artikelen";

2° au paragraphe 2, un alinéa est inséré entre les alinéas 2 et 3, rédigé comme suit:

“En cas d'urgence, le dirigeant du service ou son délégué peut décider d’accéder à ces données oralement. Cette décision est confirmée dans un délai de vingt-quatre heures par une décision écrite, selon les modalités fixées à l'alinéa 4.”.

3° au paragraphe 5, alinéa 2, le mot “enquête” est remplacé par le mot “information”;

Art. 15

Dans le Chapitre III, Section 4, Sous-section 1, il est inséré un article 16/5, rédigé comme suit:

“Art. 16/5. Les services de renseignement et de sécurité peuvent, dans l’intérêt de l’exercice de leurs missions, interagir de manière anonyme et durable dans le monde réel ou virtuel afin d’entretenir des contacts avec des personnes ou des groupements dans le but de collecter des données en rapport avec des personnes physiques, morales ou virtuelles, des associations de fait, des groupements, des objets, des lieux ou des informations.”

Art. 16

Dans le Chapitre III, Section 4, Sous-section 1, il est inséré un article 16/6 rédigé comme suit:

“Art. 16/6. § 1er. Les services de renseignement et de sécurité peuvent, dans l’intérêt de l’exercice de leurs missions, requérir le concours:

1° des personnes et institutions visées à l’article 5, paragraphe 1er, 3° à 22°, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l’utilisation des espèces;

2° des personnes et institutions qui, sur le territoire belge, mettent à disposition ou proposent des services en lien avec des valeurs virtuelles permettant d’échanger des moyens de payement réglementés en valeurs virtuelles;

3° du Point de Contact Central tenu par la Banque nationale de Belgique conformément à la loi du 8 juillet 2018 portant organisation d’un point de contact central des comptes et contrats financiers et portant extension de l’accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt;

afin de procéder à:

2° in paragraaf 2 wordt tussen het tweede en het derde lid een lid ingevoegd, luidende:

"In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde mondeling beslissen om toegang te hebben tot deze gegevens. Deze mondelinge beslissing wordt binnen vierentwintig uur bevestigd door een schriftelijke beslissing volgens de nadere regels bepaald in het vierde lid.";

3° in paragraaf 5, tweede lid worden de woorden “opsporingsonderzoek of gerechtelijk onderzoek” vervangen door de woorden “opsporings- of gerechtelijk onderzoek”.

Art. 15

In Hoofdstuk III, Afdeling 4, Onderafdeling 1, wordt een artikel 16/5 ingevoegd, luidende:

“Art. 16/5. De inlichtingen- en veiligheidsdiensten kunnen zich, in het belang van de uitoefening van hun opdrachten, op anonieme en duurzame wijze in de reële of virtuele wereld begeven teneinde contacten te onderhouden met personen of groeperingen om gegevens te verzamelen omtrent natuurlijke personen, rechtspersonen of virtuele personen, feitelijke verenigingen, groeperingen, voorwerpen, plaatsen of informatie.”

Art. 16

In Hoofdstuk III, Afdeling 4, Onderafdeling 1, wordt een artikel 16/6 ingevoegd, luidende:

“Art. 16/6. §1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van:

1° de personen en instellingen bedoeld in artikel 5, paragraaf 1, 3° tot 22° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;

2° de personen en instellingen die, binnen het Belgisch grondgebied, diensten beschikbaar stellen of aanbieden met betrekking tot virtuele waarden die toelaten dat gereglementeerde betaalmiddelen in virtuele waarden worden uitgewisseld;

3° het Centraal Aanspreekpunt gehouden door de Nationale Bank van België overeenkomstig de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van bankrekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest;

om over te gaan tot:

a) l'identification des produits et services dont la personne visée est le titulaire, le mandataire ou le bénéficiaire effectif;

b) l'identification des titulaires, des mandataires ou des bénéficiaires effectifs des produits et services.

Le dirigeant du service ou son délégué effectue la réquisition, visée au premier alinéa, 1° et 2°, par écrit. En cas d'extrême urgence, le dirigeant du service ou son délégué peut requérir ces données oralement. Cette réquisition verbale doit être confirmée par écrit dans un délai de vingt-quatre heures.

La coopération requise visée au premier alinéa, 3 ° a lieu après une décision écrite du dirigeant du service ou de son délégué, et conformément à la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt. En cas d'extrême urgence, le dirigeant du service ou son délégué peut autoriser verbalement la méthode. Cette décision verbale est confirmée par une décision écrite dans un délai de vingt-quatre heures.

§ 2. La personne ou l'institution requise est tenue de remettre sans délai les informations demandées après réception de la réquisition écrite du dirigeant du service ou de son délégué.

La personne ou l'institution requise qui refuse de prêter le concours visé au présent article est punie d'une amende de vingt-six euros à vingt mille euros.

§ 3. Les deux services de renseignement et de sécurité tiennent un registre de toutes les identifications requises. Le service de renseignement et de sécurité concerné transmet chaque mois au Comité permanent R une liste des identifications requises.

Le Comité permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans des circonstances qui ne respectent pas les conditions légales."

Art. 17

À l'article 18 de la même loi, les modifications suivantes sont apportées:

1° l'actuel alinéa 1 formera le paragraphe 1er;

a) het identificeren van de producten en diensten, waarvan de geviseerde persoon titularis, gevolmachtigde of de uiteindelijke gerechtigde is;

b) het identificeren van de titularissen, de gevolmachtigden, of de uiteindelijke gerechtigden van de producten en diensten.

De vordering bedoeld in het eerste lid, 1° en 2° gebeurt schriftelijk door het diensthoofd of zijn gedelegeerde. In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde deze gegevens mondeling vorderen. Deze mondelinge vordering wordt binnen de vierentwintig uur bevestigd door een schriftelijke vordering.

De gevorderde medewerking bedoeld in het eerste lid, 3° gebeurt na schriftelijke beslissing van het diensthoofd of zijn gedelegeerde, en overeenkomstig de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van bankrekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest. In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde de methode mondeling toestaan. Deze mondelinge beslissing wordt binnen de vierentwintig uur bevestigd door een schriftelijke beslissing.

§ 2. De gevorderde persoon of instelling is ertoe gehouden de gevraagde informatie onverwijld te verstrekken na ontvangst van de schriftelijke vordering van het diensthoofd of zijn gedelegeerde.

De gevorderde persoon of instelling die de in dit artikel bedoelde medewerking weigert te verlenen, wordt gestraft met geldboete van zesentwintig euro tot twintigduizend euro.

§ 3. Beide inlichtingen- en veiligheidsdiensten houden een register bij van alle gevorderde identificaties. Het Vast Comité I ontvangt van de betrokken inlichtingen- en veiligheidsdienst maandelijks een lijst van de gevorderde identificaties.

Het Vast Comité I verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke voorwaarden voldoen."

Art. 17

In artikel 18 van dezelfde wet, worden de volgende wijzigingen aangebracht:

1° de bestaande tekst van het eerste lid vormt paragraaf 1;

2° il est inséré un paragraphe 2, rédigé comme suit:

"§2. Pour assurer la bonne exécution des missions visées aux articles 7, 1° et 3°/1 et 11, §1er, 1° à 3° et 5°, les services de renseignement et de sécurité peuvent mettre en œuvre des méthodes de recueil de données à l'égard d'une source humaine inscrite dans le registre des sources humaines:

1° lorsqu'il y a un doute quant à sa fiabilité, discrétion ou loyauté vis-à-vis du service de renseignement et de sécurité concerné susceptible de causer une menace à l'encontre de ce service, ou

2° pour assurer la protection de la source humaine."

Art. 18

L'article 18/1 de la même loi, inséré par la loi du 4 février 2010 et modifié par la loi du 30 mars 2017, est complété par le 3° rédigé comme suit:

"3° sans préjudice des 1° et 2°, aux services de renseignement et de sécurité, dans le cadre de l'article 18, paragraphe 2.".

Art. 19

À l'article 18/2, §3, de la même loi, les modifications suivantes sont apportées:

1° au 1er alinéa, les mots "visée à l'article 3, 6°" sont remplacés par les mots "ou, en cas d'empêchement, par le membre de la commission contacté";

2° au 1er alinéa, les mots "ou le membre de la commission contacté" sont insérés entre les mots "Le président de la commission" et les mots "est tenu de fournir";

3° au alinéa 2, les mots "ou le membre de la commission contacté" sont insérés entre les mots "le président de la commission" et les mots "vérifie si les données".

Art. 20

À l'article 18/3 de la même loi, les modifications suivantes sont apportées:

1° au paragraphe 2, 2°, les mots "et dans l'hypothèse de l'article 18/1, 3°, le code identifiant de la source humaine," sont insérés entre les mots "les évènements ou les informations" et les mots "soumis à la méthode spécifique;";

;2° er wordt een paragraaf 2 ingevoegd, luidende:

"§2. Om de goede uitvoering van de opdrachten bedoeld in de artikelen 7, 1° en 3°/1 en 11, §1, 1° tot 3° en 5° te verzekeren, kunnen de inlichtingen- en veiligheidsdiensten de methoden voor het verzamelen van gegevens aanwenden ten opzichte van een menselijke bron die is ingeschreven in het register van menselijke bronnen:

1° indien er twijfel bestaat over zijn betrouwbaarheid, discretie en loyauteit tegenover de betrokken inlichtingen- en veiligheidsdienst waardoor een dreiging kan ontstaan, of

2° ter verzekering van de veiligheid van de menselijke bron."

Art. 18

Artikel 18/1 van dezelfde wet, ingevoegd door de wet van 4 februari 2010 en gewijzigd bij de wet van 30 maart 2017, wordt aangevuld met de bepaling onder 3°, luidende:

"3° onverminderd 1° en 2°, op de inlichtingen- en veiligheidsdiensten, in het kader van artikel 18, paragraaf 2.".

Art. 19

In artikel 18/2, §3, van dezelfde wet worden de volgende wijzigingen aangebracht:

1° in het eerste lid worden de woorden "bedoeld in artikel 3, 6°," vervangen door de woorden "of ,bij verhindering, het gecontacteerde lid van de commissie";

2° in het eerste lid worden de woorden "het gecontacteerde commissielid ingevoegd tussen de woorden "De voorzitter van de commissie" en de woorden "is verplicht om";

3° in het tweede lid worden de woorden "of het gecontacteerde lid" ingevoegd tussen de woorden "voorzitter van de commissie" en de woorden "na of de via deze methode".

Art. 20

In artikel 18/3 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° in paragraaf 2, 2°, worden de woorden "en in het geval van artikel 18/1, 3° de identificatiecode van de menselijke bron," ingevoegd tussen de woorden "gebeurtenissen of informatie" en de woorden "die het voorwerp uitmaken van de specifieke methode;";

2° au paragraphe 2, 9° les mots “les infractions” sont remplacés par les mots “les faits susceptibles d’être qualifiés infraction(s)”;

3° au paragraphe 3, alinéa 2, le numéro d’article “18/6/1,” est inséré entre les numéros “18/6,” et “18/7”;

4° dans le paragraphe 6, alinéa 1er, les mots “mesures, y compris le respect des principes de subsidiarité et de proportionnalité” sont remplacés par les mots “méthodes spécifiques de recueil de données, y compris le respect des principes de subsidiarité et de proportionnalité prévu à l’article 18/3, §1er”;

5° au paragraphe 6, alinéa 3, les mots “de la commission de la protection de la vie privée” sont remplacés par les mots “du Comité permanent R”;

Art. 21

À l’article 18/9, §1er, de la même loi, les modifications suivantes sont apportées:

a) le 1° est complété avant la ponctuation “;” par les mots “ou lorsqu’il existe une menace potentielle grave visée à l’article 18, paragraphe 2”;

b) le 2° est complété par les mots “ou une menace potentielle grave visée à l’article 18, paragraphe 2”.

Art. 22

À l’article 18/10 de la même loi, les modifications suivantes sont apportées:

1° au paragraphe 2, 2°, les mots “et dans l’hypothèse de l’article 18/1, 3°, le code identifiant de la source humaine,” sont insérés entre les mots “les évènements ou les informations” et les mots “faisant l’objet de la méthode exceptionnelle de recueil de données;”;

2° au paragraphe 2, 9°, les mots “les infractions” sont remplacés par les mots “les faits susceptibles d’être qualifiés infraction(s)”;

3° au paragraphe 4, alinéas 8 et 9, les mots “Si le président” sont remplacés par les mots “Si le président ou le membre de la Commission contacté”;

4° dans le paragraphe 6, alinéa 4, les mots “de la commission de la protection de la vie privée” sont remplacés par les mots “du Comité permanent R”;

2° in paragraaf 2, 9° worden de woorden “de strafbare feiten” vervangen door de woorden "de feiten die als misdrijf kunnen worden gekwalificeerd”;

3° in paragraaf 3, tweede lid, wordt het artikelnummer “18/6/1,” ingevoegd tussen de nummers “18/6,” en “18/7”;

4° in paragraaf 6, eerste lid, worden de woorden “maatregelen, hierbij inbegrepen de naleving van de principes van subsidiariteit en proportionaliteit” vervangen door de woorden “specifieke methoden voor het verzamelen van gegevens, hierbij inbegrepen de naleving van de principes van subsidiariteit en proportionaliteit bepaald in artikel 18/3, §1”;

5° in paragraaf 6, derde lid, worden de woorden “de commissie voor de bescherming van de persoonlijke levenssfeer” vervangen door de woorden “het Vast Comité I”;

Art. 21

In artikel 18/9, §1, van dezelfde wet, worden de volgende wijzigingen aangebracht:

a) de bepaling onder 1° wordt voor het leesteken “;” aangevuld met de woorden "of indien er een ernstige potentiële dreiging bestaat zoals bedoeld in artikel 18, paragraaf 2”;

b) de bepaling onder 2° wordt aangevuld met de woorden “of een ernstige potentiële dreiging bedoeld in artikel 18, paragraaf 2”.

Art. 22

In artikel 18/10 van dezelfde wet, worden de volgende wijzigingen aangebracht:

1° in paragraaf 2, 2°, worden de woorden “en in het geval van artikel 18/1, 3° de identificatiecode van de menselijke bron,” ingevoegd tussen de woorden “gebeurtenissen of informatie” en de woorden “die het voorwerp uitmaken van de uitzonderlijke methode;”;

2° in paragraaf 2, 9°, worden de woorden “de strafbare feiten” vervangen door de woorden " de feiten die als misdrijf kunnen worden gekwalificeerd”;

3° in paragraaf 4, achtste en negende lid, worden de woorden “Indien de voorzitter” vervangen door de woorden “Indien de voorzitter of het gecontacteerde commissielid”;

4° in paragraaf 6, vierde lid, worden de woorden “de commissie voor de bescherming van de persoonlijke levenssfeer” vervangen door de woorden “het Vast Comité I”;

Art. 23

L'article 18/15 de la même loi, inséré par la loi du 4 février 2010 et modifié par la loi du 30 mars 2017, est remplacé par ce qui suit:

"Art. 18/15. § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir des informations relatives aux produits, services et transactions de nature financière et aux valeurs virtuelles, concernant la personne visée, auprès:

1° des personnes et institutions visées à l'article 5, paragraphe 1er, 3° à 22° de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces;
2° des personnes et institutions qui, sur le territoire belge, mettent à disposition ou proposent des services en lien avec des valeurs virtuelles permettant d'échanger des moyens de payement réglementés en valeurs virtuelles;

3° du Point de Contact Central tenu par la Banque nationale de Belgique conformément à la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt.

§ 2. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, exiger des personnes et institutions visées au paragraphe 1er, 1° et 2° le placement sous surveillance des transactions de la personne visée.

§ 3. La coopération requise visée au paragraphe premier, 3° a lieu conformément à la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt.

La personne ou l'institution requise, visée au paragraphe premier, 1° et 2°, est tenue de remettre sans délai les informations demandées après réception de la réquisition écrite du dirigeant du service.

Cette réquisition mentionne, selon le cas, la nature de l'avis conforme de la commission, la nature de l'avis conforme du président de la commission ou la nature de l'autorisation du ministre concerné. Dans la réquisition, le service de renseignement et de sécurité concerné fournit également une description précise des informations

Art. 23

Artikel 18/15 van dezelfde wet, ingevoegd bij de wet van 4 februari 2010 en gewijzigd bij de wet van 30 maart 2017, wordt vervangen als volgt:

"Art. 18/15. § 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, informatie over de producten, diensten en verrichtingen van financiële aard en betreffende virtuele valuta, met betrekking tot de geviseerde persoon vorderen van:

1° de personen en instellingen bedoeld in artikel 5, paragraaf 1, 3° tot 22° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;
2° de personen en instellingen die, binnen het Belgisch grondgebied, diensten beschikbaar stellen of aanbieden met betrekking tot virtuele waarden die toelaten dat gereglementeerde betaalmiddelen in virtuele waarden worden uitgewisseld;

3° het Centraal Aanspreekpunt gehouden door de Nationale Bank van België overeenkomstig de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van bankrekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest.

§2. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, van de personen en instellingen bedoeld in paragraaf 1, 1° en 2° vorderen dat de verrichtingen van de geviseerde persoon onder toezicht worden geplaatst.

§ 3. De gevorderde medewerking bedoeld in paragraaf 1, 3° gebeurt overeenkomstig de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van bankrekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest.

De gevorderde persoon of instelling, bedoeld in paragraaf 1, 1° en 2°, is ertoe gehouden de gevraagde informatie onverwijld te verstrekken na ontvangst van de schriftelijke vordering van het diensthoofd.

Deze vordering vermeldt, naargelang het geval, de aard van het eensluidend advies van de commissie, de aard van het eensluidend advies van de voorzitter van de commissie of de aard van de toelating van de betrokken minister. In

Art. 24

À l'article 20 de la même loi, les modifications suivantes sont apportées:

1° au paragraphe 1er, le mot "collaboration" est remplacé par le mot "coopération";

2° au paragraphe 2, les mots "si un tel protocole existe" sont insérés entre les mots "par les ministres concernés," et les mots "; prêter leur concours".

Art. 24

In artikel 20 van dezelfde wet, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, wordt het woord "collaboration" vervangen door het woord "cooperation" in de Franstalige versie;

2° in paragraaf 2, worden de woorden "indien een dergelijk protocol bestaat" ingevoegd tussen de woorden "door de betrokken ministers," en de woorden "; hun medewerking".

Formulaire AIR - v2 – oct. 2014

Analyse d'impact de la réglementation

RiA-AiR

:: Remplissez de préférence le formulaire en ligne ria-air.fed.be
:: Contactez le Helpdesk si nécessaire ria-air@premier.fed.be
:: Consultez le manuel, les FAQ, etc. www.simplification.be

Fiche signalétique

Auteur .a.

Membre du Gouvernement compétent	Ministres de la Justice et de la Défense
Contact cellule stratégique (nom, email, tél.)	Ferre Pauwels, ferre@teamjustitie.be, 0474 87 26 75 ; Yves Beaurain, yves.beaurain@mil.be ; 0474 90 31 19
Administration compétente	SPF Justice (VSSE) et Défense (SGRS)
Contact administration (nom, email, tél.)	**VSSE (juriserv@vsse.be; 02 205 6262) – SGRS(florence.oleffe@mil.be; 02 443 1654)**

Projet .b.

Titre du projet de réglementation	Avant-projet de loi modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.
Description succincte du projet de réglementation en mentionnant l'origine réglementaire (traités, directive, accord de coopération, actualité, …), les objectifs poursuivis et la mise en œuvre.	Le présent avant-projet de loi apporte les modifications principales suivantes : 1. Elargissement des possibilités de commettre des infractions pour les agents des services de renseignement et de sécurité afin de leur permettre de commettre des infractions absolument nécessaires dans le cadre de toutes leurs missions avec l'autorisation des magistrats. 2. Modification des dispositions applicables aux identités fictives pour les agents des services de renseignement et de sécurité afin de renforcer le contrôle lorsque ces identités fictives sont utilisées pour collecter de l'information dans le cadre d'une méthode de recueil de données. 3. Possibilité pour les sources de commettre des infractions dans des conditions strictes. 4. Possibilité de pouvoir effectuer des méthodes spécifiques et exceptionnelles de recueil de données sur une source pour contrôler sa fiabilité, discrétion ou loyauté. 5. Ajout d'une compétence au Service Général du Renseignement et de la Sécurité (SGRS) afin de pouvoir mettre ses capacités Cyber au service de la Nation en cas de crise nationale de cybersécurité. 6. Introduction d'une nouvelle méthode visant le développement, par les agents des services de renseignement, de contacts durables, de manière anonyme, avec des milieux représentant une menace pour la sécurité nationale. 7. Révision de la méthode existante de collecte de données auprès des banques et des institutions financières. 8. Modifications visant à améliorer le travail quotidien dans la pratique ou à améliorer le texte. Ce projet vise un certain nombre de modifications
Analyses d'impact déjà réalisées	☐ Oui ☒ Non Si oui, veuillez joindre une copie ou indiquer la référence du document : _ _

Consultations sur le projet de réglementation .c.

Consultations obligatoires, facultatives ou informelles :	Inspecteur des finances, Secrétaire d'Etat au Budget, Comité permanent R, Conseil d'Etat, Commission BIM.

Sources utilisées pour effectuer l'analyse d'impact .d.

Statistiques, documents de référence, organisations et personnes de référence :	SPF Justice (Sûreté de l'Etat), Défence (SGRS)

Date de finalisation de l'analyse d'impact .e.

07/05/2021

Formulaire AIR - v2 – oct. 2014

Quel est l'impact du projet de réglementation sur ces 21 thèmes ?

>

Un projet de réglementation aura généralement des impacts sur un nombre limité de thèmes.

Une liste non-exhaustive de mots-clés est présentée pour faciliter l'appréciation de chaque thème.

S'il y a des **impacts positifs et / ou négatifs, expliquez-les** (sur base des mots-clés si nécessaire) et indiquez les mesures prises pour alléger / compenser les éventuels impacts négatifs.

Pour les thèmes 3, 10, 11 et 21, des questions plus approfondies sont posées.

Consultez le manuel ou contactez le helpdesk ria-air@premier.fed.be pour toute question.

Lutte contre la pauvreté .1.

Revenu minimum conforme à la dignité humaine, accès à des services de qualité, surendettement, risque de pauvreté ou d'exclusion sociale (y compris chez les mineurs), illettrisme, fracture numérique.

☐ Impact positif ☐ Impact négatif ↓ Expliquez.

☒ Pas d'impact

_ _

Égalité des chances et cohésion sociale .2.

Non-discrimination, égalité de traitement, accès aux biens et services, accès à l'information, à l'éducation et à la formation, écart de revenu, effectivité des droits civils, politiques et sociaux (en particulier pour les populations fragilisées, les enfants, les personnes âgées, les personnes handicapées et les minorités).

☐ Impact positif ☐ Impact négatif ↓ Expliquez.

☒ Pas d'impact

Égalité entre les femmes et les hommes .3.

Accès des femmes et des hommes aux ressources : revenus, travail, responsabilités, santé/soins/bien-être, sécurité, éducation/savoir/formation, mobilité, temps, loisirs, etc.

Exercice des droits fondamentaux par les femmes et les hommes : droits civils, sociaux et politiques.

1. Quelles personnes sont directement et indirectement concernées par le projet et quelle est la composition sexuée de ce(s) groupe(s) de personnes ?

   Si aucune personne n'est concernée, expliquez pourquoi.

   Les modifications apportées à la loi organique des services de renseignement et de sécurité du 30 novembre 1998 en question ne portent pas et n'ont pas d'impact sur l'égalité entre les femmes et les hommes.

↓ Si des personnes sont concernées, répondez à la question 2.

2. Identifiez les éventuelles différences entre la situation respective des femmes et des hommes dans la matière relative au projet de réglementation.

   Aucune différence identifiée_ _

↓ S'il existe des différences, répondez aux questions 3 et 4.

3. Certaines de ces différences limitent-elles l'accès aux ressources ou l'exercice des droits fondamentaux des femmes ou des hommes (différences problématiques) ? [O/N] > expliquez

   _ _

4. Compte tenu des réponses aux questions précédentes, identifiez les impacts positifs et négatifs du projet sur l'égalité des femmes et les hommes ?

   _ _

↓ S'il y a des impacts négatifs, répondez à la question 5.

5. Quelles mesures sont prises pour alléger / compenser les impacts négatifs ?

   _ _

Santé .4.

Accès aux soins de santé de qualité, efficacité de l'offre de soins, espérance de vie en bonne santé, traitements des maladies chroniques (maladies cardiovasculaires, cancers, diabètes et maladies respiratoires chroniques), déterminants de la santé (niveau socio-économique, alimentation, pollution), qualité de la vie.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Emploi .5.

Accès au marché de l'emploi, emplois de qualité, chômage, travail au noir, conditions de travail et de licenciement, carrière, temps de travail, bien-être au travail, accidents de travail, maladies professionnelles, équilibre vie privée - vie professionnelle, rémunération convenable, possibilités de formation professionnelle, relations collectives de travail.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

Modes de consommation et production .6.

Stabilité/prévisibilité des prix, information et protection du consommateur, utilisation efficace des ressources, évaluation et intégration des externalités (environnementales et sociales) tout au long du cycle de vie des produits et services, modes de gestion des organisations.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Développement économique .7.

Création d'entreprises, production de biens et de services, productivité du travail et des ressources/matières premières, facteurs de compétitivité, accès au marché et à la profession, transparence du marché, accès aux marchés publics, relations commerciales et financières internationales, balance des importations/exportations, économie souterraine, sécurité d'approvisionnement des ressources énergétiques, minérales et organiques.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Investissements .8.

Investissements en capital physique (machines, véhicules, infrastructures), technologique, intellectuel (logiciel, recherche et développement) et humain, niveau d'investissement net en pourcentage du PIB.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Recherche et développement .9.

Opportunités de recherche et développement, innovation par l'introduction et la diffusion de nouveaux modes de production, de nouvelles pratiques d'entreprises ou de nouveaux produits et services, dépenses de recherche et de développement.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

PME .10.

Impact sur le développement des PME.

1. Quelles entreprises sont directement et indirectement concernées par le projet ?
   Détaillez le(s) secteur(s), le nombre d'entreprises, le % de PME (< 50 travailleurs) dont le % de micro-entreprise (< 10 travailleurs).
   Si aucune entreprise n'est concernée, expliquez pourquoi.

   Aucune entreprise n'est concernée étant donné que ce sont des modifications dans le cadre de la loi organique des services de renseignement. Seuls les services de renseignement sont concernés.

↓ Si des PME sont concernées, répondez à la question 2.

2. Identifiez les impacts positifs et négatifs du projet sur les PME.
   N.B. les impacts sur les charges administratives doivent être détaillés au thème 11

↓ S'il y a un impact négatif, répondez aux questions 3 à 5.

3. Ces impacts sont-ils proportionnellement plus lourds sur les PME que sur les grandes entreprises ? [O/N] > expliquez

   _ _

4. Ces impacts sont-ils proportionnels à l'objectif poursuivi ? [O/N] > expliquez

   _ _

5. Quelles mesures sont prises pour alléger / compenser les impacts négatifs ?

   _ _

Charges administratives .11.

Réduction des formalités et des obligations administratives liées directement ou indirectement à l'exécution, au respect et/ou au maintien d'un droit, d'une interdiction ou d'une obligation.

↓ Si des citoyens (cf. thème 3) et/ou des entreprises (cf. thème 10) sont concernés, répondez aux questions suivantes.

1. Identifiez, par groupe concerné, les formalités et les obligations nécessaires à l'application de la réglementation.
   S'il n'y a aucune formalité ou obligation, expliquez pourquoi.

   a.

   ↓ S'il y a des formalités et des obligations dans la réglementation actuelle*, répondez aux questions 2a à 4a.

   b.

   ↓ S'il y a des formalités et des obligations dans la réglementation en projet**, répondez aux questions 2b à 4b.

2. Quels documents et informations chaque groupe concerné doit-il fournir ?

   a. _ _*

   b. _ _**

3. Comment s'effectue la récolte des informations et des documents, par groupe concerné ?

   a.

   b.

4. Quelles est la périodicité des formalités et des obligations, par groupe concerné ?

   a. _ _*

   b. _ _**

5. Quelles mesures sont prises pour alléger / compenser les éventuels impacts négatifs ?

   _ _

Énergie .12.

Mix énergétique (bas carbone, renouvelable, fossile), utilisation de la biomasse (bois, biocarburants), efficacité énergétique, consommation d'énergie de l'industrie, des services, des transports et des ménages, sécurité d'approvisionnement, accès aux biens et services énergétiques.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Mobilité .13.

Volume de transport (nombre de kilomètres parcourus et nombre de véhicules), offre de transports collectifs, offre routière, ferroviaire, maritime et fluviale pour les transports de marchandises, répartitions des modes de transport (modal shift), sécurité, densité du trafic.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Alimentation .14.

Accès à une alimentation sûre (contrôle de qualité), alimentation saine et à haute valeur nutritionnelle, gaspillages, commerce équitable.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Changements climatiques .15.

Émissions de gaz à effet de serre, capacité d'adaptation aux effets des changements climatiques, résilience, transition énergétique, sources d'énergies renouvelables, utilisation rationnelle de l'énergie, efficacité énergétique, performance énergétique des bâtiments, piégeage du carbone.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Ressources naturelles .16.

Gestion efficiente des ressources, recyclage, réutilisation, qualité et consommation de l'eau (eaux de surface et souterraines, mers et océans), qualité et utilisation du sol (pollution, teneur en matières organiques, érosion, assèchement, inondations, densification, fragmentation), déforestation.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Air intérieur et extérieur .17.

Qualité de l'air (y compris l'air intérieur), émissions de polluants (agents chimiques ou biologiques : méthane, hydrocarbures, solvants, SOx, NOx, NH3), particules fines.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Biodiversité .18.

Niveaux de la diversité biologique, état des écosystèmes (restauration, conservation, valorisation, zones protégées) , altération et fragmentation des habitats, biotechnologies, brevets d'invention sur la matière biologique, utilisation des ressources génétiques, services rendus par les écosystèmes (purification de l'eau et de l'air, …), espèces domestiquées ou cultivées, espèces exotiques envahissantes, espèces menacées.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Nuisances .19.

Nuisances sonores, visuelles ou olfactives, vibrations, rayonnements ionisants, non ionisants et électromagnétiques, nuisances lumineuses.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

_ _

Autorités publiques .20.

Fonctionnement démocratique des organes de concertation et consultation, services publics aux usagers, plaintes, recours, contestations, mesures d'exécution, investissements publics.

☐ Impact positif ☐ Impact négatif ↓ Expliquez. ☒ Pas d'impact

Cohérence des politiques en faveur du développement .21.

Prise en considération des impacts involontaires des mesures politiques belges sur les intérêts des pays en développement.

1. Identifiez les éventuels impacts directs et indirects du projet sur les pays en développement dans les domaines suivants :

- o sécurité alimentaire
- o santé et accès aux médicaments
- o travail décent
- o commerce local et international
- o revenus et mobilisations de ressources domestiques (taxation)
- o mobilité des personnes
- o environnement et changements climatiques (mécanismes de développement propre)
- o paix et sécurité

Expliquez si aucun pays en développement n'est concerné.

L'avant-projet de loi ne concerne pas les pays en développement. L'avant-projet concerne la Belgique.

↓ S'il y a des impacts positifs et/ou négatifs, répondez à la question 2.

2. Précisez les impacts par groupement régional ou économique (lister éventuellement les pays). Cf. manuel

_ _

↓ S'il y a des impacts négatifs, répondez à la question 3.

3. Quelles mesures sont prises pour les alléger / compenser les impacts négatifs ?

_ _

Regelgevingsimpactanalyse

RiA-AiR

:: Vul het formulier bij voorkeur online in ria-air.fed.be
:: Contacteer de helpdesk indien nodig ria-air@premier.fed.be
:: Raadpleeg de handleiding, de FAQ, enz. www.vereenvoudiging.be

Beschrijvende fiche

Auteur .a.

Bevoegd regeringslid	Minister van Justitie, Minister van Defensie
Contactpersoon beleidscel (Naam, E-mail, Tel. Nr.)	**Ferre Pauwels, ferre@teamjustitie.be, 0474 87 26 75 ; Yves Beaurain, yves.beaurain@mil.be ; 0474 90 31 19**
Overheidsdienst	FOD Justitie (VSSE) en Defensie (ADIV)
Contactpersoon overheidsdienst (Naam, E-mail, Tel. Nr.)	VSSE (juriserv@vsse.be; 02 205 6262) – ADIV (pieter.vanmalderen@mil.be"; 443 1754)"

Ontwerp .b.

Titel van het ontwerp van regelgeving	Voorontwerp van wet houdende regeling van de inlichtingen- en veiligheidsdiensten
Korte beschrijving van het ontwerp van regelgeving met vermelding van de oorsprong (verdrag, richtlijn, samenwerkingsakkoord, actualiteit, …), de beoogde doelen van uitvoering.	**Dit wetsontwerp voorziet hoofdzakelijk de volgende wijzigingen:** **1. Uitbreiding van de mogelijkheden om strafbare feiten te plegen voor de agenten van de inlichtingendiensten in het kader van hun opdrachten** **2. Wijziging van modaliteiten voor het gebuik van een fictieve identiteit voor de agenten en bepalingen voor de controle op het gebruik ervan** **3. De mogelijkheid om menselijke bronnen te controleren via inzet van bijzindere inlichtingenmethodes.** **4. De mogelijkheid voor menselijke bronnen om in bepaalde gevallen overtredingen te kunnen begaan.** **5. Toevoegen van een bevoegdheid voor de ADIV in geval van een nationale cyberveiligheidscrisis** **6. Invoer van een nieuwe methode die de agenten van de inlichtingendiensten toelaat om op anonieme wijze duurzame contacten uit te bouwen met milieus die een dreiging inhouden voor de nationale veiligheid** **7. Herziening van de bestaande methode voor het verzamelen van gegevens bij banken en financiële instellingen** **8. Wijzigingen om de dagelijkse werking te verbeteren of om de wettekst te verbeteren**
Impactanalyses reeds uitgevoerd	☐ Ja ☒ Nee — Indien ja, gelieve een kopie bij te voegen of de referentie van het document te vermelden: _ _

Raadpleging over het ontwerp van regelgeving .c.

Verplichte, facultatieve of informele raadplegingen:	Inspecteur van financien, Staatssecretaris van begroting, Vast Comité I, Raad van State, BIM-commissie

Bronnen gebruikt om de impactanalyse uit te voeren .d.

Statistieken, referentiedocumenten, organisaties en contactpersonen:	FOD Justitie (VSSE), Defensie (ADIV)

Datum van beëindiging van de impactanalyse .e.

07/05/2021

Welke impact heeft het ontwerp van regelgeving op deze 21 thema's?

>

Een ontwerp van regelgeving zal meestal slechts impact hebben op enkele thema's.

Een niet-exhaustieve lijst van trefwoorden is gegeven om de inschatting van elk thema te vergemakkelijken.

Indien er een **positieve en/of negatieve impact** is, leg deze uit (gebruik indien nodig trefwoorden) en vermeld welke maatregelen worden genomen om de eventuele negatieve effecten te verlichten/te compenseren.

Voor de thema's 3, 10, 11 en 21, worden meer gedetailleerde vragen gesteld.

Raadpleeg de handleiding of contacteer de helpdesk ria-air@premier.fed.be indien u vragen heeft.

Kansarmoedebestrijding .1.

Menswaardig minimuminkomen, toegang tot kwaliteitsvolle diensten, schuldenoverlast, risico op armoede of sociale uitsluiting (ook bij minderjarigen), ongeletterdheid, digitale kloof.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Gelijke Kansen en sociale cohesie .2.

Non-discriminatie, gelijke behandeling, toegang tot goederen en diensten, toegang tot informatie, tot onderwijs en tot opleiding, loonkloof, effectiviteit van burgerlijke, politieke en sociale rechten (in het bijzonder voor kwetsbare bevolkingsgroepen, kinderen, ouderen, personen met een handicap en minderheden).

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

Gelijkheid van vrouwen en mannen .3.

Toegang van vrouwen en mannen tot bestaansmiddelen: inkomen, werk, verantwoordelijkheden, gezondheid/zorg/welzijn, veiligheid, opleiding/kennis/vorming, mobiliteit, tijd, vrije tijd, etc.

Uitoefening door vrouwen en mannen van hun fundamentele rechten: burgerlijke, sociale en politieke rechten.

1. Op welke personen heeft het ontwerp (rechtstreeks of onrechtstreeks) een impact en wat is de naar geslacht uitgesplitste samenstelling van deze groep(en) van personen?

   Indien geen enkele persoon betrokken is, leg uit waarom.

   De voorgestelde wijzigingen aan de Wet houdende de regeling van de inlichtingen- en veiligheidsdiensten van 30 november 1998 hebben geen impact op de gelijkheid tussen man en vrouw

↓ Indien er personen betrokken zijn, beantwoord dan vraag 2.

2. Identificeer de eventuele verschillen in de respectieve situatie van vrouwen en mannen binnen de materie waarop het ontwerp van regelgeving betrekking heeft.

   Geen verschillen geïdentificeerd

↓ Indien er verschillen zijn, beantwoord dan vragen 3 en 4.

3. Beperken bepaalde van deze verschillen de toegang tot bestaansmiddelen of de uitoefening van fundamentele rechten van vrouwen of mannen (problematische verschillen)? [J/N] > Leg uit

   _ _

4. Identificeer de positieve en negatieve impact van het ontwerp op de gelijkheid van vrouwen en mannen, rekening houdend met de voorgaande antwoorden?

   _ _

↓ Indien er een negatieve impact is, beantwoord dan vraag 5.

5. Welke maatregelen worden genomen om de negatieve impact te verlichten / te compenseren?

   _ _

Gezondheid .4.

Toegang tot kwaliteitsvolle gezondheidszorg, efficiëntie van het zorgaanbod, levensverwachting in goede gezondheid, behandelingen van chronische ziekten (bloedvatenziekten, kankers, diabetes en chronische ademhalingsziekten), gezondheidsdeterminanten (sociaaleconomisch niveau, voeding, verontreiniging), levenskwaliteit.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Werkgelegenheid .5.

Toegang tot de arbeidsmarkt, kwaliteitsvolle banen, werkloosheid, zwartwerk, arbeids- en ontslagomstandigheden, loopbaan, arbeidstijd, welzijn op het werk, arbeidsongevallen, beroepsziekten, evenwicht privé- en beroepsleven, gepaste verloning, mogelijkheid tot beroepsopleiding, collectieve arbeidsverhoudingen.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

Consumptie- en productiepatronen .6.

Prijsstabiliteit of -voorzienbaarheid, inlichting en bescherming van de consumenten, doeltreffend gebruik van hulpbronnen, evaluatie en integratie van (sociale- en milieu-) externaliteiten gedurende de hele levenscyclus van de producten en diensten, beheerpatronen van organisaties.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Economische ontwikkeling .7.

Oprichting van bedrijven, productie van goederen en diensten, arbeidsproductiviteit en productiviteit van hulpbronnen/grondstoffen, competitiviteitsfactoren, toegang tot de markt en tot het beroep, markttransparantie, toegang tot overheidsopdrachten, internationale handels- en financiële relaties, balans import/export, ondergrondse economie, bevoorradingszekerheid van zowel energiebronnen als minerale en organische hulpbronnen.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Investeringen .8.

Investeringen in fysiek (machines, voertuigen, infrastructuren), technologisch, intellectueel (software, onderzoek en ontwikkeling) en menselijk kapitaal, nettoinvesteringscijfer in procent van het bbp.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Onderzoek en ontwikkeling .9.

Mogelijkheden betreffende onderzoek en ontwikkeling, innovatie door de invoering en de verspreiding van nieuwe productiemethodes, nieuwe ondernemingspraktijken of nieuwe producten en diensten, onderzoeks- en ontwikkelingsuitgaven.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Kmo's .10.

Impact op de ontwikkeling van de kmo's.

1. Welke ondernemingen zijn rechtstreeks of onrechtstreeks betrokken?
   Beschrijf de sector(en), het aantal ondernemingen, het % kmo's (< 50 werknemers), waaronder het % micro-ondernemingen (< 10 werknemers).
   Indien geen enkele onderneming betrokken is, leg uit waarom.

   Geen enkele onderneming is betrokken aangezien het enkel wijzigingen aan een organieke wet van een publieke administratie betreft.

↓ Indien er kmo's betrokken zijn, beantwoord dan vraag 2.

2. Identificeer de positieve en negatieve impact van het ontwerp op de kmo's.
   N.B. De impact op de administratieve lasten moet bij thema 11 gedetailleerd worden.

↓ Indien er een negatieve impact is, beantwoord dan vragen 3 tot 5.

3. Is deze impact verhoudingsgewijs zwaarder voor de kmo's dan voor de grote ondernemingen? [J/N] > Leg uit

   _ _

4. Staat deze impact in verhouding tot het beoogde doel? [J/N] > Leg uit

   _ _

5. Welke maatregelen worden genomen om deze negatieve impact te verlichten / te compenseren?

   _ _

Administratieve lasten .11.

Verlaging van de formaliteiten en administratieve verplichtingen die direct of indirect verbonden zijn met de uitvoering, de naleving en/of de instandhouding van een recht, een verbod of een verplichting.

↓ Indien burgers (zie thema 3) en/of ondernemingen (zie thema 10) betrokken zijn, beantwoord dan volgende vragen.

1. Identificeer, per betrokken doelgroep, de nodige formaliteiten en verplichtingen voor de toepassing van de regelgeving.
   Indien er geen enkele formaliteiten of verplichtingen zijn, leg uit waarom.

   a. -

   b.

↓ Indien er formaliteiten en/of verplichtingen zijn in de huidige* regelgeving, beantwoord dan vragen 2a tot 4a.

↓ Indien er formaliteiten en/of verplichtingen zijn in het ontwerp van regelgeving**, beantwoord dan vragen 2b tot 4b.

2. Welke documenten en informatie moet elke betrokken doelgroep verschaffen?

   a. _ _*

   b. _ _**

3. Hoe worden deze documenten en informatie, per betrokken doelgroep, ingezameld?

   a.

   b.

4. Welke is de periodiciteit van de formaliteiten en verplichtingen, per betrokken doelgroep?

   a. _ _*

   b. _ _**

5. Welke maatregelen worden genomen om de eventuele negatieve impact te verlichten / te compenseren?

   _ _

Energie .12.

Energiemix (koolstofarm, hernieuwbaar, fossiel), gebruik van biomassa (hout, biobrandstoffen), energie-efficiëntie, energieverbruik van de industrie, de dienstensector, de transportsector en de huishoudens, bevoorradingszekerheid, toegang tot energiediensten en -goederen.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Mobiliteit .13.

Transportvolume (aantal afgelegde kilometers en aantal voertuigen), aanbod van gemeenschappelijk personenvervoer, aanbod van wegen, sporen en zee- en binnenvaart voor goederenvervoer, verdeling van de vervoerswijzen (modal shift), veiligheid, verkeersdichtheid.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Voeding .14.

Toegang tot veilige voeding (kwaliteitscontrole), gezonde en voedzame voeding, verspilling, eerlijke handel.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Klimaatverandering .15.

Uitstoot van broeikasgassen, aanpassingsvermogen aan de gevolgen van de klimaatverandering, veerkracht, energie overgang, hernieuwbare energiebronnen, rationeel energiegebruik, energie-efficiëntie, energieprestaties van gebouwen, winnen van koolstof.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Natuurlijke hulpbronnen .16.

Efficiënt beheer van de hulpbronnen, recyclage, hergebruik, waterkwaliteit en -consumptie (oppervlakte- en grondwater, zeeën en oceanen), bodemkwaliteit en -gebruik (verontreiniging, organisch stofgehalte, erosie, drooglegging, overstromingen, verdichting, fragmentatie), ontbossing.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Buiten- en binnenlucht .17.

Luchtkwaliteit (met inbegrip van de binnenlucht), uitstoot van verontreinigende stoffen (chemische of biologische agentia: methaan, koolwaterstoffen, oplosmiddelen, SOX, NOX, NH3), fijn stof.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Biodiversiteit .18.

Graad van biodiversiteit, stand van de ecosystemen (herstelling, behoud, valorisatie, beschermde zones), verandering en fragmentatie van de habitatten, biotechnologieën, uitvindingsoctrooien in het domein van de biologie, gebruik van genetische hulpbronnen, diensten die de ecosystemen leveren (water- en luchtzuivering, enz.), gedomesticeerde of gecultiveerde soorten, invasieve uitheemse soorten, bedreigde soorten.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Hinder .19.

Geluids-, geur- of visuele hinder, trillingen, ioniserende, niet-ioniserende en elektromagnetische stralingen, lichtoverlast.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

_ _

Overheid .20.

Democratische werking van de organen voor overleg en beraadslaging, dienstverlening aan gebruikers, klachten, beroep, protestbewegingen, wijze van uitvoering, overheidsinvesteringen.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit. ☒ Geen impact

Beleidscoherentie ten gunste van ontwikkeling .21.

Inachtneming van de onbedoelde neveneffecten van de Belgische beleidsmaatregelen op de belangen van de ontwikkelingslanden.

1. Identificeer de eventuele rechtstreekse of onrechtstreekse impact van het ontwerp op de ontwikkelingslanden op het vlak van:

- o voedselveiligheid
- o gezondheid en toegang tot geneesmiddelen
- o waardig werk
- o lokale en internationale handel
- o inkomens en mobilisering van lokale middelen (taxatie)
- o mobiliteit van personen
- o leefmilieu en klimaatverandering (mechanismen voor schone ontwikkeling)
- o vrede en veiligheid

Indien er geen enkelen ontwikkelingsland betrokken is, leg uit waarom.

Het voorontwerp heeft geen betrekking op derde landen.

↓ Indien er een positieve en/of negatieve impact is, beantwoord dan vraag 2.

2. Verduidelijk de impact per regionale groepen of economische categorieën (eventueel landen oplijsten). Zie bijlage

_ _

↓ Indien er een negatieve impact is, beantwoord dan vraag 3.

3. Welke maatregelen worden genomen om de negatieve impact te verlichten / te compenseren?

_ _

AVIS DU CONSEIL D'ÉTAT
N° 69.480/2 DU 24 JUIN 2021

Le 31 mai 2021, le Conseil d'État, section de législation, a été invité par le Vice-Premier ministre et ministre de la Justice et de la Mer du Nord à communiquer un avis, dans un délai de trente jours, sur un avant-projet de loi 'modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité'.

L'avant-projet a été examiné par la deuxième chambre le 24 juin 2021. La chambre était composée de Pierre Vandernoot, président de chambre, Patrick Ronvaux et Christine Horevoets, conseillers d'État, Sébastien Van Drooghenbroeck et Jacques Englebert, assesseurs, et Béatrice Drapier, greffier.

Le rapport a été présenté par Pauline Lagasse, auditeur, et Aurore Percy, auditeur adjoint.

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

L'avis, dont le texte suit, a été donné le 24 juin 2021.

*

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

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

Observations générales

1. L'avant-projet de loi a pour objet de modifier plusieurs dispositions de la loi du 30 novembre 1998 'organique des services de renseignement et de sécurité' (ci-après: "la loi organique").

Les mesures prescrites sont résumées comme suit dans l'exposé des motifs:

"Le présent projet de loi prévoit principalement:

1) Pour les agents des services de renseignement et de sécurité:

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

ADVIES VAN DE RAAD VAN STATE
Nr. 69.480/2 VAN 24 JUNI 2021

Op 31 mei 2021 is de Raad van State, afdeling Wetgeving, door de Vice-eersteminister en minister van Justitie en Noordzee verzocht binnen een termijn van dertig dagen een advies te verstrekken over een voorontwerp van wet 'tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten'.

Het voorontwerp is door de tweede kamer onderzocht op 24 juni 2021. De kamer was samengesteld uit Pierre Vandernoot, kamervoorzitter, Patrick Ronvaux en Christine Horevoets, staatsraden, Sébastien Van Drooghenbroeck en Jacques Englebert, assessoren, en Béatrice Drapier, griffier.

Het verslag is uitgebracht door Pauline Lagasse, auditeur, en Aurore Percy, adjunct-auditeur.

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

Het advies, waarvan de tekst hierna volgt, is gegeven op 24 juni 2021.

*

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

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

Algemene opmerkingen

1. Het voorontwerp van wet strekt tot wijziging van verscheidene bepalingen van de wet van 30 november 1998 'houdende regeling van de inlichtingen- en veiligheidsdiensten' (hierna: "de organieke wet").

In de memorie van toelichting worden de voorgeschreven maatregelen als volgt samengevat:

"Dit wetsontwerp voorziet hoofdzakelijk:

1) Voor de agenten van de inlichtingen- en veiligheidsdiensten:

[1] ‡ Aangezien het om een voorontwerp van wet gaat, wordt onder "rechtsgrond" de overeenstemming met de hogere rechtsnormen verstaan.

— un élargissement des possibilités de commettre des infractions dans le cadre de leurs missions (par exemple, dans le cadre du travail des agents virtuels);

— une procédure spécifique pour l'utilisation d'une identité fictive comme mesure d'appui à une méthode de recueil de données;

— une nouvelle méthode visant le développement, par les agents des services de renseignement, de contacts durables, de manière anonyme, avec des milieux représentant une menace pour la sécurité nationale;

2) En ce qui concerne les sources humaines:

— la possibilité pour les sources de pouvoir commettre des infractions dans le cadre de conditions strictes;

— la possibilité de pouvoir effectuer des [méthodes spécifiques et exceptionnelles de recueil des données (BIM)] sur les sources pour contrôler leur fiabilité, leur discrétion ou leur loyauté;

3) Une compétence pour le Service Général du Renseignement et de la Sécurité (SGRS) est ajoutée en cas de crise nationale de cybersécurité;

4) Un remaniement de la méthode de collecte déjà existante auprès des institutions bancaires et financières:

— l'identification des données bancaires et financières devient une méthode ordinaire de collecte;

— un élargissement du champ d'application de la méthode exceptionnelle de collecte, conforme aux évolutions du monde financier;

5) Des modifications pour améliorer le travail quotidien dans la pratique ou pour réparer des oublis du législateur".

Il y a lieu de relever plus particulièrement que l'article 16 de l'avant-projet introduit dans la sous-section relative aux méthodes ordinaires de recueil des données un article 16/6, s'inspirant de l'article 18/5 actuel de la loi organique, qui permet aux services de renseignement et de sécurité de requérir certaines données auprès de banques et d'institutions financières.

Les articles 17 à 22 de l'avant-projet tendent, quant à eux, à permettre aux services de renseignement et de sécurité de mettre en œuvre des méthodes de recueil de données à l'égard d'une source humaine inscrite dans le registre des sources humaines lorsqu'il y a un doute quant à sa fiabilité, sa discrétion ou sa loyauté vis-à-vis du service de renseignement et de sécurité concerné susceptible de causer une menace à l'encontre de ce service ou pour assurer la protection de la source humaine en question.

La section de législation a rappelé ce qui suit dans son avis n° 59.509/4 donné sur l'avant-projet devenu la loi du 30 mars

— een uitbreiding van de mogelijkheden om strafbare feiten te plegen in het kader van hun opdrachten (bijvoorbeeld in het kader van de inzet van virtuele agenten);

— een specifieke procedure voor het gebruik van een fictieve identiteit als ondersteuningsmaatregel voor een methode voor het verzamelen van gegevens;

— een nieuwe methode die de agenten van de inlichtingendiensten toelaat om op anonieme wijze duurzame contacten uit te bouwen met milieus die een dreiging inhouden voor de nationale veiligheid;

2) Voor wat betreft de menselijke bronnen:

— De mogelijkheid voor bronnen om strafbare feiten te plegen onder strikte voorwaarden;

— De mogelijkheid om [specifieke of uitzonderlijke methoden voor het verzamelen van gegevens (BIM's)] uit te voeren op bronnen teneinde hun betrouwbaarheid, discretie of loyaliteit te controleren;

3) Er wordt een bevoegdheid voor de Algemene Dienst Inlichting en Veiligheid (ADIV) toegevoegd in geval van een nationale cyberveiligheidscrisis;

4) Een herziening van de reeds bestaande methode voor het verzamelen van gegevens bij banken en financiële instellingen:

— de identificatie van bank- en financiële gegevens wordt een gewone methode voor het verzamelen van gegevens;

— een uitbreiding van het toepassingsgebied van de uitzonderlijke methode voor het verzamelen van gegevens, overeenkomstig de veranderingen in de financiële wereld;

5) Wijzigingen om de dagelijkse werking in de praktijk te verbeteren of vergetelheden van de wetgever te corrigeren."

Er moet meer in het bijzonder op gewezen worden dat bij artikel 16 van het voorontwerp in de onderafdeling betreffende de gewone methoden voor het verzamelen van gegevens een artikel 16/6 ingevoegd wordt dat gebaseerd is op het huidige artikel 18/5 van de organieke wet dat het voor de inlichtingen- en veiligheidsdiensten mogelijk maakt om bij banken en financiële instellingen bepaalde gegevens te vorderen.

De artikelen 17 tot 22 van het voorontwerp strekken er op hun beurt toe het voor de inlichtingen- en veiligheidsdiensten mogelijk te maken om methoden voor het verzamelen van gegevens aan te wenden ten opzichte van een menselijke bron die is ingeschreven in het register van menselijke bronnen wanneer er twijfel bestaat over zijn betrouwbaarheid, discretie en loyauteit tegenover de betrokken inlichtingen- en veiligheidsdienst waardoor ten aanzien van die dienst een dreiging kan ontstaan of ter verzekering van de veiligheid van de menselijke bron in kwestie.

De afdeling Wetgeving heeft op het volgende gewezen in haar advies 59.509/4 over het voorontwerp dat geleid heeft

2017 'modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259*bis* du Code pénal':

"Les méthodes de recueil de données par les services de renseignement et de sécurité – qu'il s'agisse des méthodes exceptionnelles, spécifiques voire même ordinaires – sont, par nature, attentatoires à la vie privée et à l'exercice d'autres droits et libertés fondamentaux.

Il ne peut y être recouru que dans les cas prévus par la loi de manière suffisamment précise, en vue d'objectifs légitimes et à la condition que les restrictions aux droits et libertés fondamentaux soient proportionnées à l'objectif légitime poursuivi"[2].

Dans ce même avis, la section de législation a souligné l'annulation, par l'arrêt n° 145/2011 du 22 septembre 2011 de la Cour constitutionnelle, de l'article 2,§ 3, de la loi organique en raison du fait que, lorsque la personne concernée fait l'objet d'une méthode de recueil de données, celle-ci ne pouvait être informée de l'existence de cette méthode que par la voie d'une notification faite à sa demande et à la condition qu'elle justifie d'un intérêt légitime, et non par la voie d'une notification à l'initiative des services concernés.

La loi du 30 mars 2017 'modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259*bis* du Code pénal' entendait notamment donner suite à l'arrêt de la Cour constitutionnelle précité.

Saisie d'un recours en annulation portant notamment sur l'article 2, § 3, de la loi du 30 novembre 1998 nouvellement introduit, la Cour constitutionnelle a annulé la disposition attaquée par son arrêt n° 41/2019 du 14 mars 2019.

On peut lire ce qui suit dans les motifs de cet arrêt:

"B.9. L'article 2, § 3, alinéa 1er, de la loi du 30 novembre 1998 prévoit qu'à la requête de toute personne ayant un intérêt personnel et légitime qui relève de la juridiction belge, le dirigeant du service informe par écrit cette personne qu'elle a fait l'objet d'une méthode visée aux articles 18/12, 18/14 ou 18/17 de la loi du 30 novembre 1998.

Il s'en déduit que le mécanisme de 'notification sur demande' prévu par la disposition attaquée concerne exclusivement certaines méthodes exceptionnelles de collecte de données, à savoir (1) l'inspection de lieux non accessibles au public à l'aide ou non de moyens techniques et du contenu d'objets verrouillés ou non qui s'y trouvent, ainsi que l'enlèvement

[2] Avis n° 59.509/4 donné le 27 juin 2016 sur l'avant-projet devenu loi du 30 mars 2017 'modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259*bis* du Code pénal' (*Doc. parl.*, Chambre, 2015-2016, n° 2043/001, p. 126 à 162, *https://www.lachambre.be/FLWB/PDF/54/2043/54K2043001.pdf*).

tot de wet van 30 maart 2017 'tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst en van artikel 259*bis* van het Strafwetboek':

"De methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten – ongeacht of het gaat om de uitzonderlijke, de specifieke of zelfs de gewone methoden – tasten uit de aard der zaak de persoonlijke levenssfeer en de uitoefening van andere fundamentele rechten en vrijheden aan.

Ze mogen slechts aangewend worden in de gevallen waarin de wet op voldoende nauwkeurige wijze voorziet voor het halen van legitieme doelstellingen en op voorwaarde dat de beperkingen van de fundamentele rechten en vrijheden evenredig zijn met de nagestreefde legitieme doelstelling."[2]

In datzelfde advies heeft de afdeling Wetgeving erop gewezen dat het Grondwettelijk Hof bij arrest 145/2011 van 22 september 2011 artikel 2, § 3, van de organieke wet vernietigd heeft omdat, wanneer ten aanzien van de betrokken persoon een methode voor het verzamelen van gegevens aangewend wordt, die persoon enkel van het bestaan van die methode op de hoogte gebracht kon worden via een op zijn verzoek gedane kennisgeving en op voorwaarde dat hij doet blijken van een wettelijk belang, en niet via een kennisgeving op initiatief van de betrokken diensten.

De wet van 30 maart 2017 'tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst en van artikel 259*bis* van het Strafwetboek' strekte er onder meer toe gevolg te geven aan het voormelde arrest van het Grondwettelijk Hof.

Het Grondwettelijk Hof, waarbij een beroep tot nietigverklaring ingesteld was dat onder meer betrekking had op het pas ingevoerde artikel 2, § 3, van de wet van 30 november 1998, heeft in zijn arrest 41/2019 van 14 maart 2019 de nietigverklaring uitgesproken van de bestreden bepaling.

In de motivering van dat arrest staat het volgende te lezen:

"B.9. Artikel 2, § 3, eerste lid, van de wet van 30 november 1998 bepaalt dat, op verzoek van iedere persoon met een persoonlijk en wettig belang die onder de Belgische rechtsmacht valt, het diensthoofd die persoon schriftelijk informeert dat hij het voorwerp heeft uitgemaakt van een methode bedoeld in de artikelen 18/12, 18/14 of 18/17 van de wet van 30 november 1998.

Hieruit vloeit voort dat het mechanisme van de 'kennisgeving op verzoek' waarin de bestreden bepaling voorziet, uitsluitend betrekking heeft op bepaalde uitzonderlijke methoden voor het verzamelen van gegevens, namelijk (1) het doorzoeken van niet voor het publiek toegankelijke plaatsen, al dan niet met behulp van technische middelen en van de inhoud van al dan

[2] Advies 59.509/4, op 27 juni 2016 gegeven over een voorontwerp dat ontstaan heeft gegeven aan de wet van 30 maart 2017 'tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst en van artikel 259*bis* van het Strafwetboek' (*Parl. St.* Kamer 2015-16, nr. 2043/001, 126-162, *https://www.dekamer.be/FLWB/PDF/54/2043/54K2043001.pdf*).

de ces objets et le replacement de ceux-ci (article 18/12), (2) l'ouverture et la prise de connaissance du courrier confié ou non à un opérateur postal (article 18/14) et (3) l'interception, la prise de connaissance et l'enregistrement de communications (article 18/17). En revanche, il ne s'applique ni aux méthodes ordinaires, ni aux méthodes spécifiques, ni aux méthodes exceptionnelles visées aux articles 18/11, 18/13, 18/15 et 18/16 de la loi du 30 novembre 1998.

En outre, quatre conditions doivent être réunies pour qu'une notification puisse intervenir: (1°) une période de plus de dix ans doit s'être écoulée depuis la fin de la méthode; (2°) la notification ne peut nuire à une enquête de renseignement; (3°) aucun manquement aux obligations visées aux articles 13, alinéa 3, et 13/4, alinéa 2, ne doit avoir été commis et (4°) la notification ne peut porter atteinte aux relations que la Belgique entretient avec des États étrangers et des institutions internationales ou supranationales (article 2, § 3, alinéa 1er, *in fine*).

Lorsque le dirigeant du service constate que la requête est recevable, que la personne a fait l'objet d'une méthode visée aux articles 18/12, 18/14 ou 18/17 et que les quatre conditions pour la notification précitées sont remplies, il indique à la personne concernée la méthode mise en œuvre et sa base légale (article 2, § 3, alinéa 3). Dans le cas contraire, il informe la personne qu'il n'y a pas lieu de donner suite à sa requête (article 2, § 3, alinéa 2).

B.10. L'examen et le contrôle des méthodes de surveillance secrète peuvent intervenir à trois stades: lorsqu'on ordonne la surveillance, pendant qu'on la mène ou après qu'elle a cessé (CEDH, 13 septembre 2018, *Big brother watch et autres c. Royaume-Uni*, § 309; 19 juin 2018, *Centrum för Rättvisa c. Suède*, § 105; grande chambre, 4 décembre 2015, *Roman Zakharov c. Russie*, § 233).

En ce qui concerne le troisième stade, c'est-à-dire lorsque la surveillance a cessé, la Cour européenne des droits de l'homme a jugé:

'[…] la question de la notification *a posteriori* de mesures de surveillance est indissolublement liée à celle de l'effectivité des recours judiciaires et donc à l'existence de garanties effectives contre les abus des pouvoirs de surveillance. La personne concernée ne peut guère, en principe, contester rétrospectivement devant la justice la légalité des mesures prises à son insu, sauf si on l'avise de celles-ci (*Klass et autres*, précité, § 57, et *Weber et Saravia*, décision précitée, § 135) ou si – autre cas de figure –, soupçonnant que ses communications font ou ont fait l'objet d'interceptions, la personne a la faculté de saisir les tribunaux, ceux-ci étant compétents même si le sujet de l'interception n'a pas été informé de cette mesure (*Kennedy*, précité, § 167)' (CEDH, grande chambre, 4 décembre 2015, *Roman Zakharov c. Russie*, § 234. Voir aussi: CEDH, 13 septembre 2018, *Big brother watch et autres*

niet vergrendelde voorwerpen die zich daar bevinden, alsook het meenemen van die voorwerpen en het terugplaatsen ervan (artikel 18/12), (2) het openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post (artikel 18/14) en (3) het onderscheppen, kennisnemen en registreren van communicaties (artikel 18/17). Het is daarentegen niet van toepassing op de gewone methoden, de specifieke methoden of de uitzonderlijke methoden bedoeld in de artikelen 18/11, 18/13, 18/15 en 18/16 van de wet van 30 november 1998.

Bovendien moet worden voldaan aan vier voorwaarden opdat een kennisgeving kan gebeuren: (1°) een periode van meer dan tien jaar moet verstreken zijn sinds het beëindigen van de methode; (2°) de kennisgeving mag geen schade toebrengen aan een inlichtingenonderzoek; (3°) er mag geen afbreuk worden gedaan aan de verplichtingen bedoeld in de artikelen 13, derde lid, en 13/4, tweede lid, en (4°) de kennisgeving mag geen schade toebrengen aan de betrekkingen die België met vreemde Staten en internationale of supranationale instellingen onderhoudt (artikel 2, § 3, eerste lid, *in fine*).

Wanneer het diensthoofd vaststelt dat het verzoek ontvankelijk is, dat de persoon het voorwerp is geweest van een methode bedoeld in de artikelen 18/12, 18/14 of 18/17 en dat is voldaan aan de vier voormelde voorwaarden voor de kennisgeving, licht hij de betrokkene in over de ingezette methode en de wettelijke basis ervan (artikel 2, § 3, derde lid). In het andere geval licht hij de persoon erover in dat er geen gevolg kan worden gegeven aan zijn verzoek (artikel 2, § 3, tweede lid).

B.10. Het onderzoek en de controle van de methoden van geheim toezicht kunnen in drie fasen worden uitgevoerd: bij het bevelen van het toezicht, tijdens de tenuitvoerlegging ervan of na de stopzetting ervan (EHRM, 13 september 2018, *Big brother watch en anderen t. Verenigd Koninkrijk*, § 309; 19 juni 2018, *Centrum för Rättvisa t. Zweden*, § 105; grote kamer, 4 december 2015, *Roman Zakharov t. Rusland*, § 233).

Wat de derde fase betreft, dat wil zeggen wanneer het toezicht is stopgezet, heeft het Europees Hof voor de Rechten van de Mens geoordeeld:

'[De] kwestie van de kennisgeving *a posteriori* van maatregelen van toezicht is onlosmakelijk verbonden met die van de doeltreffendheid van de rechtsmiddelen en derhalve met het bestaan van doeltreffende waarborgen tegen misbruik van controlebevoegdheden. De betrokken persoon kan in beginsel moeilijk de buiten zijn of haar medeweten genomen maatregelen op retrospectieve wijze in rechte betwisten, tenzij die laatstgenoemde van die maatregelen op de hoogte wordt gebracht (*Klass en anderen*, voormeld, § 57, en *Weber en Saravia*, voormelde beslissing, § 135) of indien – andere hypothese – de persoon, vanuit een vermoeden dat zijn communicatie het voorwerp uitmaakt of heeft uitgemaakt van interceptie, de mogelijkheid heeft om een zaak aanhangig te maken bij een rechtbank, die bevoegd is zelfs indien de persoon die het voorwerp is van interceptie niet van die maatregel op

c. Royaume-Uni, § 310; 19 juin 2018, *Centrum för Rättvisa c. Suède*, § 106).

B.11. Lorsqu'elles mettent en balance l'intérêt de l'État défendeur à protéger la sécurité nationale au moyen de méthodes de surveillance secrète, d'une part, et la gravité de l'ingérence dans l'exercice du droit au respect de la vie privée, d'autre part, les autorités nationales disposent d'une certaine marge d'appréciation dans le choix des moyens propres à atteindre le but légitime que constitue la protection de la sécurité nationale (CEDH, 13 septembre 2018, *Big brother watch et autres c. Royaume-Uni*, § 308; 19 juin 2018, *Centrum för Rättvisa c. Suède*, § 104; grande chambre, 4 décembre 2015, *Roman Zakharov c. Russie*, § 232. Voir aussi: CEDH, 12 janvier 2016, *Szabó et Vissy c. Hongrie*, § 57; 18 mai 2010, *Kennedy c. Royaume-Uni*, §§ 153-154; décision, 29 juin 2006, *Weber et Saravia c. Allemagne*, § 106; 6 septembre 1978, *Klass et autres c. Allemagne*, §§ 49, 50 et 59).

Selon la jurisprudence de la Cour européenne des droits de l'homme, il incombe au premier chef aux États, conformément au principe de subsidiarité, de garantir le respect des droits et libertés définis dans la Convention, les autorités nationales, en particulier les juges nationaux, étant en principe mieux placées pour évaluer la proportionnalité d'une limitation aux droits et libertés au regard des faits et des réalités qui caractérisent la société concernée.

Il en découle que l'appréciation d'une limitation à un droit fondamental par le juge national peut conduire à ce que le niveau de protection imposé au regard de la situation nationale soit supérieur à celui que la Cour européenne des droits de l'homme prévoit.

B.12. Par son arrêt n° 145/2011 du 22 septembre 2011, la Cour a jugé que l'ancien article 2, § 3, de la loi du 30 novembre 1998, tel qu'introduit par l'article 2, 3°, de la loi du 4 février 2010, viole les articles 10 et 11 de la Constitution, lus en combinaison avec l'article 22 de celle-ci et avec l'article 8 de la Convention européenne des droits de l'homme, en ce qu'il ne prévoit de notification qu'à la requête de toute personne justifiant d'un intérêt légitime, sans prévoir qu'une notification doit également avoir lieu à l'initiative des services concernés dès l'instant où une telle notification est possible sans compromettre le but de la surveillance (B.86, B.88 et B.92).

B.13. La même conclusion s'impose pour l'article 2, § 3, de la loi du 30 novembre 1998, tel qu'il a été inséré par l'article 4, 4°, de la loi du 30 mars 2017.

B.14. En effet, la circonstance que l'ingérence dans le droit au respect de la vie privée d'une personne est effectuée à

de hoogte werd gebracht (*Kennedy*, voormeld, § 167)' (EHRM, grote kamer, 4 december 2015, *Roman Zakharov t. Rusland*, § 234. Zie ook: EHRM, 13 september 2018, *Big brother watch en anderen t. Verenigd Koninkrijk*, § 310; 19 juni 2018, *Centrum för Rättvisa t. Zweden*, § 106).

B.11. Wanneer zij de afweging maken tussen het belang van de verwerende Staat om de nationale veiligheid te beschermen door middel van methoden van geheim toezicht, enerzijds, en de ernst van de inmenging in de uitoefening van het recht op eerbiediging van het privéleven, anderzijds, beschikken de nationale autoriteiten over een zekere beoordelingsmarge voor de keuze van de middelen die geschikt zijn om het legitieme doel, namelijk de bescherming van de nationale veiligheid, te bereiken (EHRM, 13 september 2018, *Big brother watch en anderen t. Verenigd Koninkrijk*, § 308; 19 juni 2018, *Centrum för Rättvisa t. Zweden*, § 104; grote kamer, 4 december 2015, *Roman Zakharov t. Rusland*, § 232. Zie ook: EHRM, 12 januari 2016, *Szabó en Vissy t. Hongarije*, § 57; 18 mei 2010, *Kennedy t. Verenigd Koninkrijk*, §§ 153-154; beslissing, 29 juni 2006, *Weber en Saravia t. Duitsland*, § 106; 6 september 1978, *Klass en anderen t. Duitsland*, §§ 49, 50 en 59).

Volgens de rechtspraak van het Europees Hof voor de Rechten van de Mens staat het in de eerste plaats aan de Staten, overeenkomstig het subsidiariteitsbeginsel, de naleving te waarborgen van de rechten en vrijheden neergelegd in het Verdrag, omdat de nationale autoriteiten, in het bijzonder de nationale rechters, in principe beter geplaatst zijn om de evenredigheid van een beperking van de rechten en vrijheden te beoordelen in het licht van de feiten en de realiteit die de betrokken samenleving kenmerken.

Daaruit volgt dat de beoordeling van een beperking van een grondrecht door de nationale rechter ertoe kan leiden dat het beschermingsniveau in het licht van de nationale situatie hoger is dan die waarin het Europees Hof voor de Rechten van de Mens voorziet.

B.12. Bij zijn arrest nr. 145/2011 van 22 september 2011, heeft het Hof geoordeeld dat het vroegere artikel 2, § 3, van de wet van 30 november 1998, zoals ingevoegd bij artikel 2, 3°, van de wet van 4 februari 2010, de artikelen 10 en 11 van de Grondwet, in samenhang gelezen met artikel 22 ervan en met artikel 8 van het Europees Verdrag voor de rechten van de mens, schendt in zoverre het slechts voorziet in een kennisgeving op verzoek van iedere persoon die doet blijken van een wettelijk belang, zonder te bepalen dat een kennisgeving eveneens dient te gebeuren op initiatief van de betrokken diensten zodra een dergelijke kennisgeving mogelijk is zonder dat het doel van het toezicht in het gedrang wordt gebracht (B.86, B.88 en B.92).

B.13. Dezelfde conclusie geldt voor artikel 2, § 3, van de wet van 30 november 1998, zoals ingevoegd bij artikel 4, 4°, van de wet van 30 maart 2017.

B.14. De omstandigheid dat de inmenging in het recht op eerbiediging van het privéleven van een persoon buiten zijn

son insu en augmente la gravité, ce qui implique qu'elle soit entourée des garanties les plus élevées.

La circonstance qu'une méthode de surveillance secrète a pris fin ne fait pas disparaitre l'ingérence importante dans le droit au respect de la vie privée de cette personne. Une certaine information donnée *a posteriori* à la personne ne fait pas davantage disparaître cette ingérence. En effet, le fait qu'elle en ait été informée ne signifie pas qu'elle y ait consenti.

B.15.1. Comme la Cour l'a jugé par l'arrêt n° 145/2011 (B.86), la question de la notification ultérieure de méthodes de surveillance est indissociablement liée au caractère effectif des recours juridictionnels et donc à l'existence de garanties effectives contre les abus; s'il n'est pas avisé des méthodes appliquées à son insu, l'intéressé ne peut guère, en principe, en contester rétrospectivement la légalité en justice.

L'absence de notification *a posteriori* aux personnes touchées par des méthodes de surveillance secrète, dès la levée de celles-ci, ne saurait en soi justifier la conclusion que l'ingérence n'est pas conforme aux normes de référence citées en B.2, car c'est précisément cette absence d'information qui assure l'efficacité de la méthode constitutive de l'ingérence.

En revanche, il y a lieu d'aviser la personne concernée après la levée des méthodes de surveillance dès que la notification peut être donnée sans compromettre le but de la restriction.

B.15.2. La notification d'une méthode de surveillance secrète sert à informer la personne concernée qu'elle a fait l'objet d'une telle mesure, ainsi que des fondements qui l'ont motivée, le cas échéant pour permettre à cette personne de contester la légalité de la méthode en justice en connaissance de cause.

À défaut de notification active, la possibilité pour les justiciables qui ont fait l'objet d'une mesure de surveillance secrète d'avoir accès à un organe juridictionnel pour contester la légalité de celle-ci est uniquement théorique. En effet, en vertu de la disposition attaquée, les personnes soumises à certains types de méthodes exceptionnelles de collecte de données reçoivent notification du fait qu'elles ont fait l'objet d'une telle méthode uniquement à la suite de la requête d'information qu'elles adressent d'initiative au dirigeant du service et si les conditions énumérées en B.9 sont réunies. Parmi celles-ci figurent l'exigence que la requête soit recevable et celle qu'un délai de plus de dix ans se soit écoulé depuis la fin de la méthode. Il est toutefois peu probable qu'une personne qui n'a pas été informée du fait qu'elle a fait l'objet d'une mesure de surveillance secrète cherche à vérifier d'initiative

medeweten gebeurt, verhoogt immers de ernst ervan, hetgeen impliceert dat de hoogste waarborgen eraan dienen te worden verbonden.

Het gegeven dat een methode van geheim toezicht is beëindigd, doet de aanzienlijke inmenging in het recht op eerbiediging van het privéleven van die persoon niet verdwijnen. Zekere informatie die aan de persoon *a posteriori* wordt meegedeeld, doet die inmenging evenmin verdwijnen. Het feit dat hij ervan op de hoogte is gebracht, betekent immers niet dat hij ermee heeft ingestemd.

B.15.1. Bij zijn arrest nr. 145/2011 (B.86) heeft het Hof geoordeeld dat de kwestie van de latere kennisgeving van toezichtsmethoden onlosmakelijk is verbonden met het daadwerkelijke karakter van de jurisdictionele beroepen en dus met het bestaan van daadwerkelijke waarborgen tegen misbruik; wanneer de betrokkene niet wordt ingelicht over de buiten zijn weten toegepaste methoden, kan hij in beginsel de wettigheid ervan moeilijk op retrospectieve wijze in rechte betwisten.

De ontstentenis van een kennisgeving *a posteriori* aan de personen die zijn getroffen door methoden van geheim toezicht, zodra die methoden zijn opgeheven, kan op zich het besluit niet verantwoorden dat de inmenging niet in overeenstemming is met de in B.2 vermelde referentienormen, daar het precies die afwezigheid van informatie is die de doeltreffendheid verzekert van de maatregel die een inmenging vormt.

De betrokken persoon dient daarentegen te worden ingelicht na de opheffing van de toezichtsmethoden zodra de kennisgeving kan gebeuren zonder het doel van de beperking in het gedrang te brengen.

B.15.2. De kennisgeving van een methode van geheim toezicht heeft tot doel de betrokken persoon in te lichten over het feit dat hij het voorwerp heeft uitgemaakt van een dergelijke methode, alsook over de gronden welke die methode hebben gemotiveerd, teneinde die persoon in voorkomend geval in staat te stellen de wettigheid van de methode met kennis van zaken in rechte te betwisten.

Bij ontstentenis van een actieve kennisgeving is de mogelijkheid voor de rechtzoekenden die het voorwerp hebben uitgemaakt van een methode van geheim toezicht om toegang te hebben tot een jurisdictioneel orgaan teneinde de wettigheid ervan te betwisten, louter theoretisch. Krachtens de bestreden bepaling ontvangen de personen die aan bepaalde soorten van uitzonderlijke methoden voor het verzamelen van gegevens zijn onderworpen, immers alleen een kennisgeving van het feit dat zij het voorwerp hebben uitgemaakt van een dergelijke methode na het verzoek om informatie dat zij op eigen initiatief richten aan het diensthoofd en indien is voldaan aan de in B.9 opgesomde voorwaarden. Twee daarvan zijn de vereiste dat het verzoek ontvankelijk is en de vereiste dat een termijn van meer dan tien jaar verstreken is na het einde van een methode. Het is evenwel weinig waarschijnlijk dat een

et à intervalles réguliers si elle a ou non fait l'objet d'une telle méthode plus de dix ans auparavant.

B.15.3. Dès lors que la levée du secret est un préalable indispensable à l'exercice d'un recours effectif contre une méthode de surveillance secrète, il appartient au législateur de prévoir un mécanisme de notification active par lequel l'organe qu'il désigne porte à la connaissance de la personne concernée qu'elle a fait l'objet d'une méthode de surveillance secrète, dès que cette notification peut être donnée sans compromettre le but de la restriction. […]".

Compte tenu de ce que l'avant-projet de loi à l'examen introduit de nouvelles méthodes de collecte de renseignements et entend également réparer des oublis du législateur, la section de législation attire l'attention de l'auteur de l'avant-projet sur la nécessité qui demeure encore d'adapter le dispositif de la loi organique afin de se conformer à la jurisprudence de la Cour constitutionnelle et de la Cour européenne des droits de l'homme précitée.

2. À de nombreuses reprises, l'avant-projet prévoit qu'en cas d'extrême urgence, le dirigeant du service demande l'accord verbal préalable du président de la Commission ou, en cas d'indisponibilité, d'un autre membre (voir notamment les articles 13/1, § 5, 13/2, § 2, alinéa 4, et 18/2, § 3, en projet de la loi organique).

Le commentaire de l'article 13/1 en projet de la loi organique (article 5 de l'avant-projet) précise qu'

"[u]n service de renseignement et de sécurité ne peut contacter un autre membre de la commission que lorsque le président n'est pas joignable. Le choix du membre à contacter dans ce cas est préalablement déterminé par la Commission BIM elle-même et communiqué aux services. Par conséquent, les services de renseignement et de sécurité ne peuvent pas choisir quel autre membre ils peuvent contacter dans le cadre de la procédure d'urgence".

Une telle obligation de désignation préalable par la Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données des services de renseignement et de sécurité, dite "commission BIM", constitue effectivement une garantie d'un fonctionnement indépendant et impartial de ses membres et de la commission elle-même.

L'auteur de l'avant-projet veillera à imposer à la Commission de déterminer, dans son règlement d'ordre intérieur, l'ordre dans lequel les membres de la Commission doivent intervenir pour suppléer l'indisponibilité du président pour l'ensemble des hypothèses envisagées par la loi organique telle qu'elle serait modifiée par l'avant-projet.

persoon die niet erover ingelicht is dat hij het voorwerp heeft uitgemaakt van een methode van geheim toezicht op eigen initiatief en op regelmatige tijdstippen tracht na te gaan of hij al dan niet het voorwerp heeft uitgemaakt van een dergelijke methode meer dan tien jaar geleden.

B.15.3. Aangezien de opheffing van het geheim een onontbeerlijke voorwaarde is voor de uitoefening van een daadwerkelijk beroep tegen een maatregel van geheim toezicht, staat het aan de wetgever te voorzien in een mechanisme van actieve kennisgeving waarmee het door hem aangewezen orgaan de betrokkene ervan in kennis stelt dat hij het voorwerp heeft uitgemaakt van een maatregel van geheim toezicht, zodra die kennisgeving kan gebeuren zonder het doel van de beperking in het gedrang te brengen. (…)"

Gelet op het feit dat het voorliggende voorontwerp van wet nieuwe methoden voor het verzamelen van inlichtingen invoert en er tevens toe strekt vergetelheden van de wetgever recht te zetten, wijst de afdeling Wetgeving de steller van het voorontwerp erop dat het nog steeds nodig is om het dispositief van de organieke wet aan te passen ter wille van de overeenstemming met de voormelde rechtspraak van het Grondwettelijk Hof en van het Europees Hof voor de Rechten van de Mens.

2. In het voorontwerp wordt meermaals bepaald dat het diensthoofd in geval van hoogdringendheid vooraf het mondeling akkoord vraagt van de voorzitter van de Commissie of, bij onbereikbaarheid, van een ander lid (zie inzonderheid de ontworpen artikelen 13/1, § 5, 13/2, § 2, vierde lid, en 18/2, § 3, van de organieke wet).

In de bespreking van het ontworpen artikel 13/1 van de organieke wet (artikel 5 van het voorontwerp) staat het volgende:

"Enkel wanneer de voorzitter niet kan gecontacteerd worden, kan een inlichtingen- en veiligheidsdienst een ander lid van de commissie contacteren. De keuze van het desgevallend te contacteren lid wordt vooraf bepaald door de BIM-Commissie zelf, en meegedeeld aan de diensten. De inlichtingen- en veiligheidsdiensten kunnen bijgevolg niet kiezen welk ander lid ze kunnen contacteren binnen de hoogdringendheidsprocedure."

Die verplichting voor de bestuurlijke Commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten, de zogenaamde "BIM-Commissie", om vooraf iemand aan te wijzen vormt wel degelijk een waarborg voor een onafhankelijke en onpartijdige werking van de leden van de Commissie en van de Commissie zelf.

De steller van het voorontwerp moet erop toezien dat de Commissie verplicht wordt om in haar huishoudelijk reglement de volgorde te bepalen waarin de leden van de Commissie de onbereikbaarheid van de voorzitter moeten opvangen in alle gevallen voorzien in de organieke wet zoals ze bij het voorontwerp gewijzigd zou worden.

Examen de l'avant-projet

Dispositif

Article 2

1. Dans la phrase liminaire, les mot et chiffre "Art. 2." seront omis et les mots "modifiée par les lois du 6 décembre 2015, 29 janvier 2016 et 21 avril 2016" seront remplacés par les mots "modifié en dernier lieu par la loi du 30 mars 2017".

2. À l'article 2, 1°, il y a lieu de préciser si la modification s'applique à la première occurrence du mot "commission" ou aux deux occurrences de ce mot.

3. L'article 2, 3°, qui modifie l'article 3, 9°, b), de la loi organique, tend à permettre à tout agent de niveau A du Service Général du Renseignement et de la Sécurité (ci-après: "le SGRS") d'être désigné en qualité d'officier de renseignement. L'article 3, 9°, a), de la loi organique, qui prévoit que, pour la Sûreté de l'État, seul l'agent revêtu du grade de commissaire au moins peut être désigné en qualité d'officier de renseignement, n'est pas modifié.

Le commentaire de cet article expose ce qui suit à ce sujet:

"La modification apportée à l'article 3, 9°, b) est nécessaire pour permettre à tous les membres civils du personnel de niveau A du SGRS de demander et de suivre la mise en œuvre d'une méthode de recueil de données spécifique ou exceptionnelle (= BIM), alors qu'à l'heure actuelle, seuls les officiers et les commissaires sont habilités à le faire et donc pas les civils niveau A statutaires CAMU, ni les civils niveau A contractuels.

La garantie quant à l'exigence du grade de commissaire n'est pas affectée par la modification, celle-ci a pour objet d'appliquer la même garantie pour les différents statuts civils, en exigeant la désignation de civils de niveaux A.

L'objectif est d'élargir la réserve de personnel interne dans laquelle le SGRS pourra sélectionner des personnes susceptibles de devenir des officiers de renseignement.

Il n'entre pas dans la volonté du SGRS de multiplier les désignations d'officiers de renseignement mais simplement d'élargir la réserve de personnel interne. Trois officiers de renseignement sont désignés actuellement".

Le commentaire de l'article ne permet pas d'expliquer pourquoi l'élargissement de la catégorie d'agents qui peuvent être désignés en qualité d'officiers de renseignement est limité au Service Général du Renseignement et de la Sécurité, à l'exclusion de la Sûreté de l'État.

L'auteur de l'avant-projet doit être en mesure de justifier la différence de traitement créée entre les agents de niveau A du SGRS, d'une part, et les agents de niveau A de la Sûreté

Onderzoek van het voorontwerp

Dispositief

Artikel 2

1. In de inleidende zin moeten het woord en het cijfer "Art. 2." weggelaten worden en moeten de woorden "gewijzigd bij de wetten van 6 december 2015, 29 januari 2016 en 21 april 2016" vervangen worden door de woorden "laatstelijk gewijzigd bij de wet van 30 maart 2017".

2. In artikel 2, 1°, moet verduidelijkt worden of de wijziging geldt voor de eerste vermelding van het woord "commissie" dan wel voor beide vermeldingen van dat woord.

3. Artikel 2, 3°, waarbij artikel 3, 9°, b), van de organieke wet gewijzigd wordt, strekt ertoe het voor elke agent van niveau A van de Algemene Dienst Inlichting en Veiligheid (hierna: "de ADIV") mogelijk te maken om tot inlichtingenofficier aangewezen te worden. Er wordt geen wijziging aangebracht in artikel 3, 9°, a), van de organieke wet, dat bepaalt dat, wat de Veiligheid van de Staat betreft, enkel de agent die ten minste de graad van commissaris heeft tot inlichtingenofficier aangewezen kan worden.

In de bespreking van dat artikel wordt in dat verband het volgende gesteld:

"De wijziging aangebracht in artikel 3, 9°, b) is noodzakelijk om het burgerpersoneel van niveau A van de ADIV de mogelijkheid te bieden om de aanwending van een specifieke of uitzonderlijke methode (een zogeheten BIM-methode) voor het verzamelen van gegevens te vorderen en op te volgen, terwijl nu alleen de officieren en commissarissen, en dus niet de burgerambtenaren van niveau A met een CAMU-statuut, daartoe gemachtigd zijn.

De wijziging raakt niet aan de waarborg inzake de vereiste graad van commissaris; ze strekt ertoe dezelfde waarborg toe te passen voor de verschillende burgerstatuten door de aanstelling van burgerambtenaren van niveaus A te vereisen.

Het is de bedoeling om de interne personeelsreserve waaruit de ADIV personen kan selecteren om inlichtingenofficier te worden, uit te breiden.

De ADIV heeft niet de intentie de aanwijzing van inlichtingenofficiers te vermenigvuldigen, maar wil alleen de interne personeelsreserve uitbreiden. Momenteel zijn er drie inlichtingenofficieren aangewezen."

De bespreking van het artikel kan niet verklaren waarom de uitbreiding van de categorie van agenten die als inlichtingenofficier aangewezen kunnen worden zich beperkt tot de Algemene Dienst Inlichting en Veiligheid, met uitsluiting van de Veiligheid van de Staat.

De steller van het voorontwerp moet het verschil in behandeling kunnen rechtvaardigen dat ontstaat tussen de agenten van niveau A van de ADIV enerzijds en de agenten

de l'État, d'autre part, dans la mesure où les premiers pourront être désignés en qualité d'officier de renseignement même s'ils ne sont pas revêtus du grade de commissaire, alors que, s'agissant des seconds, seuls les agents de niveau A revêtus du grade de commissaire pourront être officiers de renseignement.

Article 3

1. Dans la phrase liminaire, il y a lieu d'indiquer les modifications encore en vigueur de l'article modifié[3].

La même observation vaut pour les articles 17 à 22 de l'avant-projet.

2. Dans le texte français du 1°, il sera précisé que les mots "des conflits armés" sont remplacés par le mot "international" dans les deux versions linguistiques. Dans le texte néerlandais on indiquera que les mots "het recht van de gewapende conflicten" sont remplacés par les mots "het internationaal recht".

3. Les mots "intérêts vitaux du pays ou les besoins essentiels de la population", qui figurent au 5°, sont définis comme suit dans le commentaire de l'article:

"Il faut entendre par 'intérêts vitaux du pays ou les besoins essentiels de la population' auxquels renvoie cette notion:

– l'ordre public, c'est-à-dire la tranquillité, la salubrité et la sécurité publiques;

– le potentiel scientifique et économique du pays;

– la souveraineté nationale et les institutions établies par la Constitution et les lois;

– l'intégrité du territoire national".

Cette définition s'inspire de celle qui figure à l'article 2, § 2, de l'arrêté royal du 18 avril 1988 'portant création du Centre gouvernemental de Coordination et de Crise'.

Il y a lieu de faire figurer cette définition dans la loi.

4. Dans la version française du 4°, il y a lieu de fermer les guillemets après le texte de l'article 11, § 2, 5°, en projet de la loi du 30 novembre 1998.

Article 4

Il y a lieu d'indiquer les articles que comprend la nouvelle sous-section.

[3] *Principes de technique législative - Guide de rédaction des textes législatifs et réglementaires, www.raadvst-consetat.be*, onglet "Technique législative", recommandation n° 113.

van niveau A van de Veiligheid van de Staat anderzijds, in zoverre de eerstgenoemden tot inlichtingenofficier aangewezen zullen kunnen worden ook al hebben ze niet de graad van commissaris, terwijl, wat de laatstgenoemden betreft, enkel de agenten van niveau A die de graad van commissaris hebben inlichtingenofficier zullen kunnen zijn.

Artikel 3

1. In de inleidende zin moet melding gemaakt worden van de nog geldende wijzigingen van het artikel dat gewijzigd wordt.[3]

Dezelfde opmerking geldt voor de artikelen 17 tot 22 van het voorontwerp.

2. In de Nederlandse tekst van de bepaling onder 1° moet aangegeven worden dat de woorden "het recht van de gewapende conflicten" vervangen moeten worden door de woorden "het internationaal recht". In de Franse tekst van diezelfde bepaling schrijve men dat de woorden "des conflits armés" vervangen moeten worden door het woord "international".

3. De in de bepaling onder 5° vervatte woorden "vitale belangen van het land of de essentiële behoeften van de bevolking" worden als volgt gedefinieerd in de bespreking van het artikel:

"Onder 'vitale belangen van het land of essentiële behoeften van de bevolking' waarnaar dit begrip verwijst, moet het volgende worden begrepen:

– de openbare orde, dat wil zeggen de openbare rust, gezondheid en veiligheid;

– het wetenschappelijk en economisch potentieel van het land;

– de nationale soevereiniteit en de instellingen opgericht bij de Grondwet en de wetten;

– de integriteit van het nationaal grondgebied."

Deze definitie is gebaseerd op die welke vervat is in artikel 2, § 2, van het koninklijk besluit van 18 april 1988 'tot oprichting van het [C]oördinatie- en Crisiscentrum van de regering'.

Die definitie moet in de wet opgenomen worden.

4. In de Franse tekst van de bepaling onder 4° moet het aanhalingsteken gesloten worden na de tekst van het ontworpen artikel 11, § 2, 5°, van de wet van 30 november 1998.

Artikel 4

Er dient aangegeven te worden welke artikelen deel uitmaken van de nieuwe onderafdeling.

[3] *Beginselen van de wetgevingstechniek - Handleiding voor het opstellen van wetgevende en reglementaire teksten, http://www .raadvst-consetat.be* Wetgevingstechniek", aanbeveling 113.

La même observation vaut pour les articles 8, 10 et 11.

ARTICLE 5

1. Dans la version française du 2°, les mots “à l’alinéa” seront remplacés par les mots “à l’alinéa 1er”.

2. L’article 5, 2°, tend à remplacer les mots “la méthode” par les mots “leur mission” dans l’article 13/1, § 2, de la loi organique.

Comme l’expliquent les délégués du ministre, dès lors que les membres de l’équipe d’intervention n’exécutent pas de méthode, l’intention de l’auteur de l’avant-projet est d’englober, dans le terme “mission”, la méthode exécutée par les agents et la mission réalisée par les membres de l’équipe d’intervention.

Pour transcrire fidèlement l’intention de l’auteur de l’avant-projet et ne pas donner l’impression que l’on modifie la portée de l’article 13/1, § 2, en ce qui concerne les agents chargés d’exécuter les méthodes de recueil de données, mieux vaudrait remplacer l’article 13/1, § 2, par ce qui suit:

“Par dérogation au paragraphe 1er, sont exemptés de peine les agents chargés d’exécuter les méthodes de recueil de données qui commettent des contraventions, des infractions au code de la route ou un vol d’usage, qui sont absolument nécessaires afin d’assurer l’exécution optimale de la méthode ou de garantir leur propre sécurité ou celle de tiers. De même, sont exemptés de peine les membres de l’équipe d’intervention dans le cadre de leur fonction qui commettent des contraventions, des infractions au code de la route ou un vol d’usage, qui sont absolument nécessaires afin d’assurer l’exécution optimale de leur mission ou de garantir leur propre sécurité ou celle de tiers”.

ARTICLE 6

1. Dans la phrase liminaire, les mots “par l’article 6” seront remplacés par les mots “par l’article 4”.

La même observation vaut pour l’article 7.

2. L’article 13/1/1, § 2, alinéa 4, 4°, en projet prévoit que le dirigeant du service mentionne dans sa demande “la synthèse de l’analyse de risque(s) sur les faits susceptibles d’être qualifiés infraction(s)”.

L’auteur de l’avant-projet précisera, à tout le moins, les finalités de cette analyse de risque(s) et le moment auquel elle doit être réalisée, le cas échéant en introduisant une disposition générale prévoyant que l’analyse de risque(s) doit

Dezelfde opmerking geldt voor de artikelen 8, 10 en 11.

ARTIKEL 5

1. In de Franse tekst van de bepaling onder 2° moeten de woorden “à l’alinéa” vervangen worden door de woorden “à l’alinéa 1er”.

2. Artikel 5, 2°, strekt ertoe in artikel 13/1, § 2, van de organieke wet de woorden “de methode” te vervangen door de woorden “hun opdracht”.

De gemachtigden van de minister leggen uit dat het, aangezien de leden van het interventieteam geen methode uitvoeren, de bedoeling van de steller van het voorontwerp is om met het woord “opdracht” zowel de methode uitgevoerd door de agenten als de opdracht uitgevoerd door de leden van het interventieteam te omvatten.

Teneinde de bedoeling van de steller van het voorontwerp getrouw weer te geven en niet de indruk te wekken dat met betrekking tot de agenten belast met de uitvoering van de methoden voor het verzamelen van gegevens een wijziging aangebracht wordt in de strekking van artikel 13/1, § 2, zou deze laatste bepaling beter door de volgende tekst vervangen worden:

“In afwijking van paragraaf 1, blijven vrij van straf de agenten belast met de uitvoering van de methoden voor het verzamelen van gegevens die overtredingen, inbreuken op de wegcode of een gebruiksdiefstal plegen die strikt noodzakelijk zijn voor het welslagen van de methode of ter verzekering van hun eigen veiligheid of die van derden. Zo ook blijven vrij van straf de leden van het interventieteam in het kader van hun functie, die overtredingen, inbreuken op de wegcode of een gebruiksdiefstal plegen die strikt noodzakelijk zijn voor het welslagen van hun opdracht of ter verzekering van hun eigen veiligheid of die van derden.”

ARTIKEL 6

1. In de inleidende zin moeten de woorden “bij artikel 6” vervangen worden door de woorden “bij artikel 4”.

Dezelfde opmerking geldt voor artikel 7.

2. Het ontworpen artikel 13/1/1, § 2, vierde lid, 4°, bepaalt dat de vraag van het diensthoofd melding maakt van “de synthese van de risicoanalyse over de beoogde feiten die als misdrijf kunnen worden gekwalificeerd”.

De steller van het voorontwerp moet op zijn minst preciseren wat de bedoeling is van die risicoanalyse en op welk ogenblik ze uitgevoerd moet worden, in voorkomend geval door een algemene bepaling in te voegen waarin gesteld wordt dat de

être réalisée préalablement à toute mesure de protection et d'appui[4].

3. Comme l'indiquent les délégués du ministre, l'article 13/1/1, § 5, en projet, s'applique sans préjudice d'autres obligations qui restent applicables à la source humaine même en cas d'extrême urgence, telle l'obligation de signer un mémorandum qui précise notamment les conditions strictes à respecter par la source humaine lorsqu'elle commet l'infraction.

L'article 13/1/1, § 5, en projet sera revu afin d'indiquer les subdivisions de l'article 13/1/1 qui restent applicables à la source humaine dans la procédure d'extrême urgence.

4. L'article 6, § 9, alinéa 3, en projet, de la loi organique prévoit que

"[l]a source humaine suit les directives du service de renseignement et de sécurité concerné dans la négociation de l'indemnisation ou la gestion du contentieux. Les modalités pratiques sont précisées dans le mémorandum visé au § 3. Si les directives ne sont pas respectées, l'État peut refuser l'indemnisation ou n'en prendre qu'une partie en charge".

Interrogés sur la portée de cette disposition, les délégués du ministre ont expliqué qu'en cas de dommage subi ou causé par la source humaine lors de la commission d'une infraction autorisée, l'indemnisation sera prise en charge par l'État, sans que celui-ci puisse intervenir dans le processus de négociation ou être partie à la cause en cas de procédure judiciaire. L'objectif est ne pas révéler la qualité de "source humaine" afin de garantir la sécurité de la source humaine et de ne pas compromettre la réussite de l'opération menée par les services de renseignements et de sécurité. Il se justifierait, dans ces conditions, que ces derniers puissent donner des "directives" à la source humaine dans le processus d'indemnisation.

De telles directives sont susceptibles d'entraîner une dérogation à la loi du 22 août 2002 'relative aux droits du patient' et, plus généralement, de restreindre les droits fondamentaux de la source humaine, tels que le principe d'égalité et de non-discrimination, le droit au respect de la vie privée, qui

[4] L'article 2, § 1er, *in fine*, de la loi organique prévoit qu'il est tenu compte des risques dans l'examen du principe de subsidiarité mais cette disposition s'applique uniquement aux méthode spécifiques ou exceptionnelles de recueil de données.

risicoanalyse vóór elke beschermings- en ondersteuningsmaatregel uitgevoerd moet worden.[4]

3. Zoals door de gemachtigden van de minister aangegeven wordt, geldt het ontworpen artikel 13/1/1, § 5, onverminderd andere verplichtingen die zelfs in geval van hoogdringendheid op de menselijke bron van toepassing blijven, zoals de verplichting om een memorandum te ondertekenen waarin onder meer de strikte voorwaarden bepaald worden die door de menselijke bron nageleefd moeten worden bij het plegen van het strafbaar feit.

Het ontworpen artikel 13/1/1, § 5, moet aldus herzien worden dat daarin de onderverdelingen van artikel 13/1/1 vermeld worden die in de hoogdringendheidsprocedure van toepassing blijven op de menselijke bron.

4. Het ontworpen artikel 6, § 9, derde lid, van de organieke wet luidt als volgt:

"De menselijke bron volgt de richtlijnen van de betrokken inlichtingen- en veiligheidsdienst bij de onderhandelingen over de schadeloosstelling of de afhandeling van het geschil. De praktische modaliteiten zijn bepaald in het memorandum bedoeld in § 3. Indien de richtlijnen niet nageleefd worden, kan de Staat de schadeloosstelling weigeren of deze slechts gedeeltelijk ten laste nemen."

Gevraagd naar de strekking van die bepaling hebben de gemachtigden van de minister toegelicht dat, in geval van schade die door de menselijke bron bij het plegen van een toegestaan strafbaar feit geleden of aangericht wordt, de schadeloosstelling door de Staat ten laste genomen zal worden, zonder dat deze laatste bij de onderhandelingsprocedure betrokken kan worden of betrokken partij kan zijn in geval van een gerechtelijke procedure. Het is de bedoeling om de hoedanigheid van de "menselijke bron" niet kenbaar te maken teneinde de veiligheid van de menselijke bron te garanderen en het welslagen van de door de inlichtingen- en veiligheidsdiensten gevoerde operatie niet in gevaar te brengen. In die omstandigheden zou het gerechtvaardigd zijn dat deze diensten tijdens de schadeloosstellingsprocedure "richtlijnen" kunnen geven aan de menselijke bron.

Dergelijke richtlijnen kunnen een afwijking van de wet van 22 augustus 2002 'betreffende de rechten van de patiënt' met zich meebrengen en kunnen meer in het algemeen tot een beperking leiden van de grondrechten van de menselijke bron, zoals het gelijkheids- en non-discriminatiebeginsel, het recht

[4] Artikel 2, § 1, *in fine*, van de organieke wet bepaalt dat bij de evaluatie van het subsidiariteitsprincipe rekening gehouden wordt met de risico's, maar die bepaling geldt enkel voor de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens.

implique notamment le droit à l'intégrité physique[5], ou le droit au procès équitable et, plus spécifiquement, le droit à l'égalité des armes qui implique notamment que chaque partie doit se voir offrir une possibilité raisonnable de présenter sa cause dans des conditions qui ne la placent pas dans une situation de désavantage par rapport à son adversaire[6]. Par conséquent, il revient à l'auteur de l'avant-projet de déterminer, à tout le moins, les finalités précises poursuivies par ces directives, de préciser les dérogations aux droits du patient et, plus largement, aux droits fondamentaux de la source humaine qui sont ainsi autorisées et de garantir le respect des principes de nécessité et de proportionnalité qui encadrent toute restriction à un droit fondamental au regard de chacune de ces finalités. L'auteur de l'avant-projet veillera à distinguer les hypothèses selon que l'indemnisation concerne le dommage causé à un tiers ou le dommage subi par la source.

ARTICLE 12

L'article 12, 1°, rend applicable aux tiers qui commettent des infractions le régime d'indemnisation prévu, pour les sources humaines, par l'article 13/1/1, § 9, de la loi organique.

Comme le confirment les délégués du ministre, l'article 13/1/1, § 9, ne peut être appliqué *mutatis mutandis* aux tiers dans la mesure où ces derniers ne doivent pas signer de memorandum avant de commettre une infraction et où la demande d'autorisation déposée par le dirigeant du service ne doit pas

[5] Il résulte de la jurisprudence de la Cour européenne des droits de l'homme que le corps d'une personne représente l'aspect le plus intime de la vie privée. Ainsi, une intervention médicale forcée, même mineure, constitue une ingérence dans l'exercice du droit au respect de la vie privée garanti par l'article 8 de la Convention européenne des droits de l'homme. Par conséquent, le droit à l'intégrité physique implique le droit de choisir de suivre un traitement médical et le libre choix du médecin ou de l'institution hospitalière: voir notamment Cour eur. D.H., *Solomakhin c. Ukraine*, 15 mars 2012, § 33; *Vavricka et autres c. République tchèque*, 8 avril 2021, § 263.
On relève à cet égard qu'il a été jugé qu'une réglementation par laquelle, afin de constater l'admission au bénéfice des allocations de chômage, l'appréciation de l'incapacité de travail du chômeur n'est pas laissée à son médecin personnel, mais est confiée à des médecins désignés par l'autorité, qui prennent à cet égard une décision suivant une procédure déterminée, n'est pas une immixtion dans le droit au respect de la vie privée garanti par l'article 8 de la Convention européenne des droits de l'homme. (Cass., 23 juin 1980, *Pa*s., 1980, I, p. 130*3; R*.W., 1980-1981, col. 446 et note P. LEMMENS). La loi du 10 avril 1971 'sur les accidents du travail' organise également un mécanisme d'évaluation de l'incapacité par un médecin-conseil. Les limitations quant au libre choix du médecin consulté sont cependant encadrées précisément par la loi et se limitent à l'évaluation de l'incapacité.

[6] Voir notamment Cour eur. D.H., *Bulut c. Autriche*, 22 février 1996, § 47; *Faig Mammadov c. Azerbaïdjan*, 26 janvier 2017, § 19.

op eerbiediging van het privéleven, dat onder meer het recht op lichamelijke integriteit inhoudt,[5] of het recht op een eerlijk proces en, meer specifiek, het recht op wapengelijkheid, dat onder meer inhoudt dat elke partij over de redelijke mogelijkheid moet beschikken om haar zaak uiteen te zetten in zodanige omstandigheden dat ze niet in een situatie verzeilt waarin ze in het nadeel is ten opzichte van haar tegenpartij.[6] Bijgevolg moeten door de steller van het voorontwerp op zijn minst de precieze doelstellingen bepaald worden die met die richtlijnen nagestreefd worden, moeten de aldus toegestane afwijkingen van de rechten van de patiënt en meer in het algemeen van de grondrechten van de menselijke bron gepreciseerd worden en moet de naleving gegarandeerd worden van het noodzakelijkheids- en het evenredigheidsbeginsel die alle beperkingen van een grondrecht afbakenen in het licht van elk van die doelstellingen. De steller van het voorontwerp moet erop toezien dat de gevallen waarin de schadeloosstelling betrekking heeft op de schade toegebracht aan een derde onderscheiden worden van de gevallen waarin ze betrekking heeft op de schade geleden door de bron.

ARTIKEL 12

Bij artikel 12, 1°, wordt de schadeloosstellingsregeling waarin artikel 13/1/1, § 9, van de organieke wet voor de menselijke bronnen voorziet, toepasselijk gemaakt op derden die strafbare feiten plegen.

De gemachtigden van de minister bevestigen dat artikel 13/1/1, § 9, niet *mutatis mutandis* op derden toegepast kan worden in zoverre die laatstgenoemden geen memorandum moeten ondertekenen voordat ze een strafbaar feit plegen en voor zover in de door het diensthoofd ingediende

[5] Uit de rechtspraak van het Europees Hof voor de Rechten van de Mens volgt dat het menselijk lichaam het meest intieme aspect van het privéleven vormt. Een gedwongen medische ingreep, hoe klein ze ook is, vormt dan ook een inmenging in de uitoefening van het recht op eerbiediging van het privéleven dat gewaarborgd wordt door artikel 8 van het Europees Verdrag voor de rechten van de mens. Bijgevolg impliceert het recht op lichamelijke integriteit het recht om ervoor te kiezen om een medische behandeling te volgen alsook de vrije keuze van de arts of van de ziekenhuisinstelling: zie onder meer EHRM 15 maart 2012, *Solomakhin t. Oekraïne*, § 33; 8 april 2021, *Vavricka e.a. t. Tsjechische Republiek*, § 263.
In dat verband moet opgemerkt worden dat geoordeeld is dat er geen sprake is van een inmenging in het door artikel 8 van het EVRM gewaarborgde recht op eerbiediging van het privéleven in geval van een regeling waarbij, voor de vaststelling van het recht op werkloosheidsuitkering, de beoordeling van de arbeidsongeschiktheid van de werkloze niet aan diens behandelende arts wordt overgelaten, maar wordt opgedragen aan artsen die door de overheid zijn aangewezen en die daarover volgens een vastgestelde procedure beslissen (Cass. 23 juni 1980, *Pa*s. 1980, I, 130*3; RW* 1980-81, col. 446 en noot P. LEMMENS). De Arbeidsongevallenwet van 10 april 1971 voorziet eveneens in een regeling waarbij de ongeschiktheid door een adviserend arts beoordeeld wordt. De beperkingen wat de vrije keuze van de geraadpleegde arts betreft worden echter nauwkeurig door de wet afgebakend en hebben louter betrekking op de beoordeling van de ongeschiktheid.

[6] Zie onder meer EHRM 22 februari 1996, *Bulut t. Oostenrijk*, § 47; 26 januari 2017, *Faig Mammadov t. Azerbeidzjan*, § 19.

préciser les conditions strictes imposées au tiers lors de la réalisation de l'infraction.

L'article 12, 1°, de l'avant-projet doit être revu afin de prévoir un régime spécifique pour l'indemnisation des dommages qui résultent des infractions commises par les tiers.

ARTICLE 13

Au 2°, la concordance entre les versions française et néerlandaise de l'article 16/3, § 2, alinéa 2, en projet de la loi organique sera mieux assurée en déplaçant, dans la version française, l'adverbe "verbalement" entre les mots "décider" et "d'accéder".

La même observation vaut pour l'article 16/4, § 2, de la même loi, en projet à l'article 14, 2°, de l'avant-projet.

ARTICLE 19

L'article 19, 1° à 3°, tend notamment à ajouter, à l'article 18/2, § 3, alinéa 1er et 2, de la loi organique, les mots "ou le membre de la commission contacté".

De l'accord des délégués du ministre, les mots "membre de la commission contacté" ne sont pas adéquats dès lors que le président et les membres de la commission ne sont pas "contactés" dans le cadre de la procédure décrite à cet article.

L'article 19 de l'avant-projet sera dès lors revu afin de refléter plus adéquatement l'intervention du membre de la commission.

En outre, afin d'assurer la cohérence de l'article 18/2, § 3, de la loi organique, l'alinéa 3 sera également modifié pour prévoir l'hypothèse où le président de la commission serait absent et où un autre membre de la commission aurait remplacé en conséquence celui-ci.

ARTICLE 21

1. Au *littera* a), les mots "ou lorsqu'il existe une menace potentielle grave visée à l'article 18, paragraphe 2" seront remplacés par les mots "ou, dans le cadre de la mise en œuvre des méthodes de recueil de données visée à l'article 18, § 2, lorsqu'il existe une menace potentielle grave liée à une source humaine".

2. Au *littera* b), les mots "ou une menace potentielle grave visée à l'article 18, paragraphe 2" seront remplacés par les mots "ou, dans le cadre de la mise en œuvre des méthodes de recueil de données visée à l'article 18, § 2, une menace potentielle grave liée à une source humaine".

machtigingsaanvraag niet de strikte voorwaarden vermeld moeten worden die aan een derde opgelegd worden bij het plegen van het strafbaar feit.

Artikel 12, 1°, van het voorontwerp moet aldus herzien worden dat het in een specifieke regeling voorziet voor de schadeloosstelling van de schade die voortvloeit uit de door derden gepleegde strafbare feiten.

ARTIKEL 13

In de bepaling onder 2° moet de Franse tekst van het ontworpen artikel 16/3, § 2, tweede lid, van de organieke wet beter afgestemd worden op de Nederlandse tekst ervan door in de Franse tekst het bijwoord "verbalement" tussen de woorden "décider" en "d'accéder" te plaatsen.

Dezelfde opmerking geldt voor het ontworpen artikel 16/4, § 2, van dezelfde wet dat vervat is in artikel 14, 2°, van het voorontwerp.

ARTIKEL 19

Artikel 19, 1° tot 3°, strekt er inzonderheid toe aan artikel 18/2, § 3, eerste en tweede lid, van de organieke wet de woorden "of het gecontacteerde lid van de Commissie" toe te voegen.

De gemachtigden van de minister zijn het ermee eens dat de woorden "het gecontacteerde lid van de Commissie" geen geschikte woorden zijn, aangezien de voorzitter en de leden van de Commissie niet "gecontacteerd" worden in het kader van de procedure die in dat artikel beschreven wordt.

Artikel 19 van het voorontwerp moet dan ook herzien worden teneinde adequater weer te geven welke rol het lid van de Commissie daarin speelt.

Teneinde voor de interne samenhang te zorgen van artikel 18/2, § 3, van de organieke wet moet het derde lid bovendien ook aldus gewijzigd worden dat het in het geval voorziet waarin de voorzitter van de Commissie afwezig zou zijn en een ander lid van de Commissie hem bijgevolg vervangen zou hebben.

ARTIKEL 21

1. In de bepaling onder a) moeten de woorden "of indien er een ernstige potentiële dreiging bestaat zoals bedoeld in artikel 18, paragraaf 2" vervangen worden door de woorden "of, in het kader van de in artikel 18, § 2, bedoelde uitvoering van de methoden voor het verzamelen van gegevens, indien er een ernstige potentiële dreiging bestaat die verband houdt met een menselijke bron".

2. In de bepaling onder b) moeten de woorden "of een ernstige potentiële dreiging bedoeld in artikel 18, paragraaf 2" vervangen worden door de woorden "of, in het kader van de in artikel 18, § 2, bedoelde uitvoering van de methoden voor het verzamelen van gegevens, een ernstige potentiële dreiging die verband houdt met een menselijke bron".

Article 24

La version française du 1° doit préciser que c'est la version française de l'article 20, § 1er, de la loi organique qui fait l'objet de la modification en projet.

Signature

Compte tenu de la portée de l'avant-projet et de l'article 6, § 2, 1°, de la loi organique, l'avant-projet doit également être signé par la ministre de la Défense et par la ministre de l'Intérieur.

Le greffier, *Le président,*

Béatrice DRAPIER Pierre VANDERNOOT

Artikel 24

In de Franse tekst van de bepaling onder 1° moet gepreciseerd worden dat het de Franse tekst van artikel 20, § 1, van de organieke wet is die bij het ontwerp gewijzigd wordt.

Ondertekening

Gelet op de strekking van het voorontwerp en artikel 6, § 2, 1°, van de organieke wet, moet het voorontwerp ook door de minister van Defensie en door de minister van Binnenlandse Zaken ondertekend worden.

De griffier, *De voorzitter,*

Béatrice DRAPIER Pierre VANDERNOOT

PROJET DE LOI

PHILIPPE,

ROI DES BELGES,

À tous, présents et à venir,

SALUT.

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

NOUS AVONS ARRÊTÉ ET ARRÊTONS:

Article 1er

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

Art. 2

À l'article 3 de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, modifié en dernier lieu par la loi du 30 mars 2017, les modifications suivantes sont apportées:

1° La version française de la disposition 4° est complété par les mots "des Forces armées";

2° dans la disposition 6°, la première mention du mot "commission" est remplacé par le mot "Commission";

3° une disposition 8°/1 est insérée, rédigée comme suit:

"8°/1 "son délégué": l'agent, autre que le gestionnaire du dossier, désigné par décision écrite du dirigeant du service transmise au Comité permanent R, pour prendre habituellement certaines décisions à la place du dirigeant du service;";

4° dans la disposition 9°, les mots"l'officier de renseignement" sont remplacés par les mots "l'officier des méthodes".

5° l'article est complété par les dispositions 22° à 28°, rédigées comme suit:

22° "faux nom": un nom qui n'appartient pas à l'agent et qui n'est pas attesté par une carte d'identité, un

WETSONTWERP

FILIP,

KONING DER BELGEN,

Aan allen die nu zijn en hierna wezen zullen,

ONZE GROET.

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

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

Artikel 1

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

Art. 2

In artikel 3 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, laatstelijk gewijzigd bij de wet van 30 maart 2017, worden de volgende wijzigingen aangebracht:

1° De Franse versie van bepaling onder 4° wordt aangevuld met de woorden "*des Forces Armées*";

2° in de bepaling onder 6° wordt de eerste vermelding van het woord "commissie" vervangen door het woord "Commissie";

3° er wordt een bepaling onder 8°/1 ingevoegd, luidende:

"8°/1 "zijn gedelegeerde": de agent, andere dan de dossierbeheerder, aangesteld door middel van een schriftelijke beslissing van het diensthoofd die overgemaakt werd aan het Vast Comité I, om gewoonlijk bepaalde beslissingen in de plaats van het diensthoofd te nemen;";

4° in de bepaling onder 9° worden de woorden "de inlichtingenofficier" vervangen door de woorden "de methodenofficier".

5° het artikel wordt aangevuld met de bepalingen 22° tot 28°, luidende:

22° "valse naam": een naam die niet toebehoort aan de agent en die niet wordt aangetoond door middel van een

passeport, une carte d'étranger ou un document de séjour ou par des documents officiels en découlant;

23° "fausse qualité": une qualité qui n'appartient pas à l'agent et dont il ne découle aucun effet juridique;

24° "identité fictive": une fausse identité attestée par une carte d'identité, un passeport, une carte d'étranger ou un document de séjour;

25° "qualité fictive": un statut, un titre ou une fonction n'appartenant pas à l'agent dont il découle des effets juridiques;

26° "source humaine": une personne qui donne une information aux services de renseignement et de sécurité et qui est enregistrée conformément à la procédure prévue dans la directive portant sur le recours à des sources humaines approuvées par le Conseil national de sécurité;

27° "s'infiltrer": le fait pour un agent, en dehors des cas visés à l'article 18, de s'intégrer délibérément dans un groupe ou dans la vie d'une personne afin de recueillir des informations ou des données, dans le cadre d'une enquête d'un service de renseignement et de sécurité et dans l'intérêt de l'exercice de ses missions, soit dans le monde virtuel, soit dans le monde réel. Cet agent dissimule sa qualité d'agent des services de renseignement et de sécurité et, pour les agents du Service Général du Renseignement et de la Sécurité, de membre du Ministère de la Défense, et:

a) participe ou facilite les activités ou soutient activement les convictions ou les activités de la personne ou du groupe qui fait l'objet de l'enquête, ou

b) entretient des relations durables avec ceux-ci.

Art. 3

À l'article 11 de la même loi, modifié en dernier lieu par la loi du 30 mars 2017, les modifications suivantes sont apportées:

1° au paragraphe 1er, f), dans la version néerlandaise, les mots "*bedreigt of zou kunnen bedreigen;*" sont déplacés à la ligne suivante;

2° au paragraphe 1er, 2°, dans la version néerlandaise, le mot "*beheerst*" est remplacé par le mot "*beheert*" et

identiteitskaart, een paspoort, een vreemdelingenkaart of een verblijfsdocument of door officiële documenten die hieruit voortvloeien;

23° "valse hoedanigheid": een hoedanigheid die niet toekomt aan de agent en waaruit geen rechtsgevolg voortvloeit;

24° "fictieve identiteit": een valse identiteit, die wordt aangetoond door middel van een identiteitskaart, een paspoort, een vreemdelingenkaart of een verblijfsdocument;

25° "fictieve hoedanigheid": een statuut, een titel of een functie die niet toebehoort aan de agent en waaruit rechtsgevolgen voortvloeien;

26° "menselijke bron": een persoon die een inlichting meedeelt aan de inlichtingen- en veiligheidsdiensten en die geregistreerd is overeenkomstig de procedure beschreven in de door de Nationale Veiligheidsraad goedgekeurde richtlijn betreffende het beroep op menselijke bronnen;

27° "infiltreren": de handeling waarbij een agent, buiten de gevallen bedoeld in artikel 18, zich doelbewust in een groep of in het leven van een persoon integreert om informatie of gegevens te verzamelen in het kader van een onderzoek van een inlichtingen- en veiligheidsdienst en in het belang van de uitoefening van zijn opdrachten, hetzij in de virtuele wereld, hetzij in de reële wereld. Deze agent verbergt zijn hoedanigheid van agent van de inlichtingen- en veiligheidsdiensten en, voor de agenten van de Algemene Dienst Inlichting en Veiligheid, van lid van het ministerie van Defensie, en:

a) neemt deel aan de activiteiten of faciliteert deze of ondersteunt actief de overtuigingen of de activiteiten van de persoon of de groep die het voorwerp uitmaakt van het onderzoek, of

b) onderhoudt duurzame contacten met hen.

Art. 3

In artikel 11 van dezelfde wet, laatstelijk gewijzigd bij de wet van 30 maart 2017, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, f) worden in de Nederlandse versie de woorden "bedreigt of zou kunnen bedreigen;" verplaatst naar het begin van de volgende regel;

2° in paragraaf 1, 2°, in de Nederlandstalige versie wordt het woord "beheerst" vervangen door het woord

les mots “des conflits armés” sont remplacés par le mot “international”;

3° au paragraphe 1er, est inséré un 2°/1 rédigé comme suit:

“2°/1 de neutraliser, dans le cadre d’une crise nationale de cybersécurité, une cyberattaque de systèmes informatiques et de communications non gérés par la Défense et d’en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit international;”

4° au paragraphe 1er, 4° et 5°, le signe de ponctuation “.” est remplacé par le signe de ponctuation “;”;

5° le paragraphe 1er est complété par le 6° rédigé comme suit:

“6° d’exécuter toutes autres missions qui lui sont confiées par ou en vertu de la loi.”

6° le paragraphe 2 est complété par le 5° rédigé comme suit:

“5° “crise nationale de cybersécurité”: tout incident de cybersécurité qui, par sa nature ou ses conséquences:

— menace les intérêts vitaux du pays ou les besoins essentiels de la population;

— requiert des décisions urgentes; et

— demande une action coordonnée de plusieurs départements et organismes.”

7° au paragraphe 3, alinéa 1er, les mots “paragraphe 1er, 1°, 2°, 3° et 5°“ sont remplacés par les mots ”paragraphe 1er, 1° à 3°, 5° et 6°”.

Art. 4

L’article 13 de la même loi, modifié en dernier lieu par la loi du 30 mars 2017, est modifié comme suit:

1° l’actuel alinéa 1er formera le paragraphe 1er;

2° l’actuel alinéa 2 formera le paragraphe 2;

3° l’actuel alinéa 3 formera le paragraphe 3;

“beheert” en worden de woorden “recht van de gewapende conflicten” vervangen door de woorden “internationaal recht”;

3° in paragraaf 1 wordt een bepaling 2°/1 ingevoegd, luidende:

“2°/1 het neutraliseren, in het kader van een nationale cybersecurity crisis, van een cyberaanval op informatica- en verbindingssystemen niet beheerd door de minister van Landsverdediging en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het internationaal recht;”

4° in paragraaf 1, 4° en 5°, wordt het leesteken”.“vervangen door het leesteken “;”;

5° paragraaf 1 wordt aangevuld met de bepaling onder 6°, luidende:

“6° het uitvoeren van alle andere opdrachten die hem door of krachtens de wet worden toevertrouwd.”

6° paragraaf 2 wordt aangevuld met de bepaling onder 5°, luidende:

“5° “nationale cybersecurity crisis”: elke cybersecurity gebeurtenis die wegens haar aard of gevolgen:

— de vitale belangen van het land of de essentiële behoeften van de bevolking bedreigt;

— een dringende besluitvorming vereist; en

— de gecoördineerde inzet van verscheidene departementen en organismen vergt.”

7° in paragraaf 3, eerste lid, worden de woorden “paragraaf 1, 1°, 2°, 3° en 5°“ vervangen door de woorden ”paragraaf 1, 1° tot 3°, 5° en 6°”.

Art. 4

Artikel 13 van dezelfde wet, laatstelijk gewijzigd bij de wet van 30 maart 2017, wordt gewijzigd als volgt:

1° de bestaande tekst van het eerste lid zal paragraaf 1 vormen;

2° de bestaande tekst van het tweede lid zal paragraaf 2 vormen;

3° de bestaande tekst van het derde lid zal paragraaf 3 vormen;

4° l'article est complété par un paragraphe 4 rédigé comme suit:

"§ 4. Lorsque, au cours d'une enquête ou d'une vérification de sécurité au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, un agent prend connaissance d'informations indiquant l'existence d'une menace potentielle visée aux article 7 et 8 ou contre un intérêt visé à l'article 11, il les transmet immédiatement par écrit au dirigeant de son service, ou à son délégué, en vue de leur traitement pour lutter contre ladite menace.".

Art. 5

Dans le Chapitre III, la Section 2, il est inséré une sous-section 1, rédigée comme suit: "Sous-section 1. Commission d'infractions". Cette sous-section comprend les articles 13/1, 13/1/1 et 13/1/2.

Art. 6

Dans la sous-section 1, insérée par l'article 5, à l'article 13/1, inséré par la loi du 4 février 2010 et modifié par la loi du 30 mars 2017, les modifications suivantes sont apportées:

1° l'actuel alinéa 1er formera le paragraphe 1er;

2° l'actuel alinéa 2, qui formera le paragraphe 2, est remplacé comme suit:

"§ 2. Par dérogation au paragraphe 1er, sont exemptés de peine les agents qui commettent des contraventions, des infractions au code de la route ou un vol d'usage, qui sont absolument nécessaires afin d'assurer l'exécution optimale de la mission ou de garantir leur propre sécurité ou celle de tiers, lorsque ces agents sont:

1° chargés d'exécuter les méthodes de recueil de données; ou

2° membres de l'équipe d'intervention."

3° les alinéas 3, 4, 5 et 6 sont abrogés et remplacés par les paragraphes 3, 4, 5, 6, 7, 8, 9, 10 et 11, rédigés comme suit:

"§ 3. Sans préjudice du paragraphe 2, sont exemptés de peine, les agents qui, lors de l'exécution des missions visées aux articles 7, 1° et 3°/1 et 11, § 1er, 1° à 3° et 5°,

4° het artikel wordt aangevuld met een paragraaf 4, luidende:

"§ 4. Indien een agent, tijdens een veiligheidsonderzoek of een veiligheidsverificatie in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, kennis neemt van informatie die wijst op het bestaan van een potentiële dreiging zoals bedoeld in de artikelen 7 en 8 of tegen een belang zoals bedoeld in artikel 11, maakt hij deze onmiddellijk schriftelijk over aan zijn diensthoofd of aan diens gedelegeerde, met het oog op de verwerking ervan ter bestrijding van de voormelde dreiging.".

Art. 5

In Hoofdstuk III, Afdeling 2, wordt een onderafdeling 1 ingevoegd, luidende: "Onderafdeling 1 – Het plegen van strafbare feiten". Deze onderafdeling bevat de artikelen 13/1, 13/1/1 en 13/1/2.

Art. 6

In onderafdeling 1, ingevoegd bij artikel 5, worden in artikel 13/1, ingevoegd bij de wet van 4 februari 2010 en gewijzigd bij de wet van 30 maart 2017, volgende wijzigingen aangebracht:

1° de bestaande tekst van het eerste lid zal paragraaf 1 vormen;

2° het huidige tweede lid, waarvan de tekst paragraaf 2 zal vormen, wordt vervangen als volgt:

"§ 2. In afwijking van paragraaf 1, blijven vrij van straf de agenten die overtredingen, inbreuken op de wegcode of een gebruiksdiefstal begaan die strikt noodzakelijk zijn voor het welslagen van de uitvoering van de opdracht of ter verzekering van hun eigen veiligheid of die van derden, wanneer deze agenten:

1° belast zijn met de uitvoering van de methoden voor het verzamelen van gegevens; of

2° leden zijn van het interventieteam."

3° de leden 3, 4, 5 en 6 worden opgeheven en vervangen door de paragrafen 3, 4, 5, 6, 7, 8, 9, 10 en 11, luidende:

"§ 3. Onverminderd paragraaf 2, blijven vrij van straf, de agenten die in de uitvoering van de opdrachten bedoeld in de artikelen 7, 1° en 3°/1 en 11, § 1, 1° tot 3° en 5°,

commettent des infractions absolument nécessaires afin d'assurer l'exécution optimale de leur mission ou de garantir leur propre sécurité ou celle de tiers.

Les infractions visées à l'alinéa 1er ne peuvent être commises qu'avec l'accord écrit préalable de la Commission. La Commission donne son accord écrit dans les quatre jours suivant la réception de la demande écrite et motivée du dirigeant du service.

L'accord ne peut porter sur une période supérieure à six mois, sans préjudice de la possibilité de prolonger la mesure en suivant la procédure visée à l'alinéa 2.

La demande du dirigeant du service mentionne, sous peine d'illégalité:

1° les faits susceptibles d'être qualifiés infraction(s);

2° le contexte de la demande et la finalité;

3° la liste des agents répondant au profil requis pour commettre les faits susceptibles d'être qualifiés infraction(s) visés au 1°;

4° l'absolue nécessité;

5° la proportionnalité visée au paragraphe 4;

6° la période durant laquelle la ou les infractions peuvent être commises à compter de l'accord de la Commission et la motivation de la durée de la période;

7° le cas échéant, les motifs qui justifient l'extrême urgence visée au paragraphe 6;

8° le nom du ou des agent(s) chargé(s) du suivi du déroulement de l'infraction;

9° la date de la demande;

10° la signature du dirigeant du service.

§ 4. Les infractions doivent être directement proportionnelles à l'objectif visé par la mission et ne peuvent en aucun cas porter atteinte à l'intégrité physique des personnes.

§ 5. L'agent qui assure le suivi du déroulement de l'infraction fait rapport par écrit au dirigeant du service

strafbare feiten plegen die strikt noodzakelijk zijn voor het welslagen van de uitvoering van hun opdracht of ter verzekering van hun eigen veiligheid of die van derden.

De strafbare feiten, bedoeld in het eerste lid, kunnen slechts worden gepleegd na voorafgaand schriftelijk akkoord van de Commissie. De Commissie geeft haar schriftelijk akkoord binnen de vier dagen na ontvangst van de schriftelijke en gemotiveerde vraag van het diensthoofd.

Het akkoord geldt voor een maximumtermijn van zes maanden, onverminderd de mogelijkheid om de maatregel te verlengen volgens de procedure bedoeld in het tweede lid.

De vraag van het diensthoofd vermeldt, op straffe van onwettigheid:

1° de feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd;

2° de context van de vraag en de finaliteit;

3° de lijst met agenten die beantwoorden aan het vereiste profiel om de feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd zoals bedoeld in 1° te plegen;

4° de strikte noodzakelijkheid;

5° de proportionaliteit bedoeld in paragraaf 4;

6° de periode waarbinnen het strafbaar feit of de strafbare feiten kunnen worden gepleegd, te rekenen vanaf het akkoord van de Commissie, en de motivering van de duur van deze periode;

7° in voorkomend geval, de redenen die de hoogdringendheid bedoeld in paragraaf 6 rechtvaardigen;

8° de naam van de agent(en) belast met de opvolging van het verloop van het strafbaar feit;

9° de datum van de vraag;

10° de handtekening van het diensthoofd.

§ 4. De strafbare feiten moeten in gelijke verhouding staan tot het door de opdracht nagestreefde doel en mogen in geen geval afbreuk doen aan de fysieke integriteit van personen.

§ 5. De agent belast met de opvolging van het verloop van het strafbaar feit brengt zo spoedig mogelijk na het

le plus rapidement possible après la commission de l'infraction.

Le service de renseignement et de sécurité concerné en informe la Commission par écrit dans les plus brefs délais.

Par dérogation à l'alinéa 2, si la mesure a été autorisée pour une période supérieure à deux mois, le service de renseignement et de sécurité concerné informe la Commission du déroulement de la mesure par écrit toutes les deux semaines.

À la demande motivée de la Commission, le rapport est transmis à plus courte échéance, pour autant que l'agent qui a commis l'infraction soit en sécurité pour le faire.

§ 6. En cas d'extrême urgence, le dirigeant du service demande l'accord verbal préalable du président de la Commission ou, s'il n'est pas joignable , d'un autre membre. L'auteur de l'accord en informe immédiatement les autres membres. Le dirigeant du service confirme sa demande par écrit dans les vingt-quatre heures suivant la communication de l'accord. Cette confirmation écrite comprend les mentions visées au paragraphe 3, alinéa 4. Le président ou le membre contacté confirme également son accord par écrit le plus rapidement possible. Cet accord est valable cinq jours.

§ 7. Si, en raison de circonstances imprévisibles, les faits susceptibles d'être qualifiés infraction(s) ont été commis pour lesquels la procédure prévue aux paragraphes 3 ou 6 n'a pas pu être suivie, le dirigeant du service en informe la Commission par écrit dans les plus brefs délais et au plus tard dans les vingt-quatre heures qui suivent sa prise de connaissance de la commission des faits susceptibles d'être qualifiés infraction(s). L'agent qui a commis ces faits bénéficie de l'exemption de peine si la Commission estime qu'ils étaient imprévisibles et strictement nécessaires pour assurer sa propre sécurité ou celle de tiers.

§ 8. Si la Commission ne rend pas sa décision conformément aux paragraphes 3, 6 ou 7, le dirigeant du service concerné peut saisir le Comité permanent R qui autorisera ou n'autorisera pas la commission de(s) (l') infraction(s) dans les plus brefs délais.

En cas de décision négative de la Commission en application des paragraphes 3, 6 ou 7, le dirigeant du service concerné peut saisir le Comité permanent R. Le Comité permanent R autorisera ou n'autorisera pas la commission d'infraction(s) dans les plus brefs délais.

plegen van het strafbaar feit schriftelijk verslag uit aan het diensthoofd.

De betrokken inlichtingen- en veiligheidsdienst informeert zo spoedig mogelijk schriftelijk de Commissie.

In afwijking van het tweede lid, indien de maatregel is toegestaan voor een periode langer dan twee maanden, brengt de betrokken inlichtingen- en veiligheidsdienst om de twee weken schriftelijk verslag uit aan de Commissie over het verloop van de maatregel.

Op gemotiveerd verzoek van de Commissie wordt het verslag op een kortere termijn overgemaakt, voor zover de agent die het strafbaar feit pleegde in veiligheid is.

§ 6. In geval van hoogdringendheid vraagt het diensthoofd vooraf het mondeling akkoord van de voorzitter van de Commissie of, indien hij niet bereikbaar is, van een ander lid. Diegene die het akkoord gegeven heeft, brengt de andere leden hiervan onmiddellijk op de hoogte. Het diensthoofd bevestigt zijn vraag schriftelijk binnen de vierentwintig uur na mededeling van het akkoord. Deze schriftelijke bevestiging bevat de vermeldingen bedoeld in paragraaf 3, lid 4. De voorzitter of het gecontacteerde lid bevestigt eveneens zo spoedig mogelijk schriftelijk zijn akkoord. Dit akkoord geldt voor vijf dagen.

§ 7. Indien door onvoorziene omstandigheden feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd gepleegd werden en waarvoor de procedure bedoeld in de paragrafen 3 of 6 niet gevolgd kon worden, brengt het diensthoofd dit zo spoedig mogelijk en ten laatste binnen de 24 uur vanaf zijn kennisname van het plegen van de feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd schriftelijk ter kennis van de Commissie. De agent die deze feiten heeft gepleegd blijft vrij van straf indien de Commissie oordeelt dat zij niet voorzienbaar en strikt noodzakelijk waren ter verzekering van de eigen veiligheid of die van derden.

§ 8. Indien de Commissie nalaat haar beslissing te nemen overeenkomstig de paragrafen 3, 6 of 7, kan het betrokken diensthoofd het Vast Comité I vatten, dat zo spoedig mogelijk al dan niet de toestemming zal geven om het strafbaar feit of de strafbare feiten te plegen.

In geval van een negatieve beslissing van de Commissie overeenkomstig de paragrafen 3, 6 of 7, kan het betrokken diensthoofd het Vast Comité I vatten. Het Vast Comité I zal zo spoedig mogelijk al dan niet de toestemming geven om het strafbaar feit of de strafbare

Le Comité permanent R communique sa décision au dirigeant du service et à la Commission.

§ 9. La Commission transmet sans délai tous les documents visés aux paragraphes 3 à 7 au Comité permanent R.

§ 10. Le dirigeant du service met fin à la mesure dès que possible lorsque l'absolue nécessité de commettre une infraction a disparu, lorsque la mesure n'est plus utile pour la finalité pour laquelle elle avait été demandée ou lorsqu'il a été constaté une illégalité. Il en informe dès que possible la Commission et le Comité permanent R.

Lorsque la Commission ou le Comité permanent R constate une illégalité, elle ou il en informe par écrit le dirigeant du service concerné. Ce dernier met fin à la mesure en cours ou planifiée dès que possible et confirme ensuite par écrit à la Commission et au Comité permanent R que la mesure a pris fin.

§ 11. Les membres de la Commission peuvent contrôler à tout moment la légalité des mesures.

Ils peuvent, à cet effet, avoir accès aux données relatives à la mesure, se saisir de toutes les pièces utiles et entendre les membres du service."

Art. 7

Dans le Chapitre III, Section 2, Sous-section 1, insérée par l'article 5, il est inséré un article 13/1/1, rédigé comme suit:

"Art. 13/1/1. § 1er. Il est interdit aux sources humaines de commettre des infractions.

§ 2. Par dérogation au paragraphe 1er, sont exemptées de peine les sources humaines majeures d'âge qui, dans l'intérêt de l'exercice des missions du service de renseignement et de sécurité concerné, telles que visées aux articles 7, 1° et 3°/1 et 11, § 1er, 1° à 3° et 5°, commettent des infractions absolument nécessaires afin d'assurer leur position d'information ou de garantir leur propre sécurité ou celle de tiers.

Les infractions ne peuvent être commises qu'avec l'accord écrit préalable de la Commission. La Commission donne son accord écrit dans les quatre jours suivant la réception de la demande écrite et motivée du dirigeant du service.

feiten te plegen. Het Vast Comité I deelt zijn beslissing mee aan het diensthoofd en aan de Commissie.

§ 9. De Commissie maakt alle documenten bedoeld in de paragrafen 3 tot 7 onverwijld over aan het Vast Comité I.

§ 10. Het diensthoofd beëindigt de maatregel zo snel mogelijk wanneer de absolute noodzaak om een strafbaar feit te plegen weggevallen is, wanneer de maatregel niet langer nuttig is voor het doel waarvoor hij werd aangevraagd of wanneer een onwettigheid is vastgesteld. Hij brengt zijn beslissing zo snel mogelijk ter kennis van de Commissie en het Vast Comité I.

Indien de Commissie of het Vast Comité I een onwettigheid vaststelt, brengt zij of hij het betrokken diensthoofd hier schriftelijk van op de hoogte. Deze laatste beëindigt zo snel mogelijk de geplande of lopende maatregel en bevestigt vervolgens schriftelijk aan de Commissie en aan het Vast Comité I dat de maatregel beëindigd is.

§ 11. De leden van de Commissie kunnen op elk ogenblik een controle uitoefenen op de wettigheid van de maatregelen.

Zij kunnen daartoe toegang hebben tot de gegevens met betrekking tot de maatregel, zich alle nuttige stukken toe-eigenen en de leden van de dienst horen."

Art. 7

In Hoofdstuk III, Afdeling 2, Onderafdeling 1, ingevoegd bij artikel 5, wordt een artikel 13/1/1 ingevoegd, luidende:

"Art. 13/1/1. § 1. Het is de menselijke bronnen verboden strafbare feiten te plegen.

§ 2. In afwijking van paragraaf 1, blijven vrij van straf, de meerderjarige menselijke bronnen die, in het belang van de uitoefening van de opdrachten van de betrokken inlichtingen- en veiligheidsdienst, zoals bedoeld in de artikelen 7, 1° en 3°/1 en 11, § 1, 1° tot 3° en 5°, strafbare feiten plegen die strikt noodzakelijk zijn ter verzekering van hun informatiepositie of ter verzekering van hun eigen veiligheid of die van derden.

De strafbare feiten kunnen slechts worden gepleegd na voorafgaand schriftelijk akkoord van de Commissie. De Commissie geeft haar schriftelijk akkoord binnen de vier dagen na ontvangst van de schriftelijke en gemotiveerde vraag van het diensthoofd.

L'accord ne peut porter sur une période supérieure à deux mois, sans préjudice de la possibilité de prolonger la mesure en suivant la procédure visée à l'alinéa 2.

Une analyse de risque(s) portant sur la fiabilité de la source et les risques qu'elle encourt dans le cadre de la commission de(s) (l')infraction(s) doit être réalisée préalablement à la demande du dirigeant du service.

La demande du dirigeant du service mentionne, sous peine d'illégalité:

1° le code d'identification de la source humaine;

2° les faits susceptibles d'être qualifiés infraction(s);

3° le contexte de la demande et la finalité;

4° la synthèse de l'analyse de risque(s) visée à l'alinéa 4;

5° l'absolue nécessité;

6° la proportionnalité visée au paragraphe 3;

7° les conditions strictes imposées à la source humaine;

8° la période durant laquelle la ou les infractions peuvent être commises et la motivation de la durée de la période;

9° le cas échéant, les motifs qui justifient l'extrême urgence visée au paragraphe 6;

10° le nom du ou des agent(s) chargé(s) du suivi du déroulement de l'infraction;

11° la date de la demande;

12° la signature du dirigeant du service.

§ 3. Les infractions doivent être directement proportionnelles à l'objectif visé par la mission et ne peuvent en aucun cas porter atteinte à l'intégrité physique des personnes.

§ 4. Avant que l'infraction autorisée ne puisse être commise, la source humaine signe un mémorandum contenant notamment les modalités de mise en œuvre et de rapportage. Ce mémorandum est conservé dans le dossier individuel de la source humaine.

Het akkoord geldt voor een maximumtermijn van twee maanden, onverminderd de mogelijkheid om de maatregel te verlengen volgens de procedure bedoeld in het tweede lid.

Een risicoanalyse betreffende de betrouwbaarheid van de bron en de risico's waar zij zich aan blootstelt in het kader van het plegen van het strafbaar feit of de strafbare feiten moet worden uitgevoerd voorafgaand aan de vraag van het diensthoofd.

De vraag van het diensthoofd vermeldt, op straffe van onwettigheid:

1° de identificatiecode van de menselijke bron;

2° de feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd;

3° de context van de vraag en de finaliteit;

4° de synthese van de risicoanalyse bedoeld in lid 4;

5° de strikte noodzakelijkheid;

6° de proportionaliteit bedoeld in paragraaf 3;

7° de strikte voorwaarden opgelegd aan de menselijke bron;

8° de periode tijdens dewelke strafbare feiten begaan kunnen worden en de motivering van de duur van deze periode;

9° in voorkomend geval, de redenen die de hoogdringendheid bedoeld in paragraaf 6 rechtvaardigen;

10° de naam van de agent(en) belast met de opvolging van het verloop van het strafbaar feit;

11° de datum van de vraag;

12° de handtekening van het diensthoofd.

§ 3. De strafbare feiten moeten in gelijke verhouding staan tot het door de opdracht nagestreefde doel en mogen in geen geval afbreuk doen aan de fysieke integriteit van personen.

§ 4. Vooraleer het toegelaten strafbaar feit kan worden gepleegd, ondertekent de menselijke bron een memorandum dat onder meer de modaliteiten voor de tenuitvoerlegging en de verslaggeving bevat. Dit memorandum wordt bewaard in het individueel dossier van de menselijke bron.

Le mémorandum est daté et inclut notamment les mentions suivantes:

1° le code d'identification de la source humaine;

2° la manière dont l'infraction sera mise en œuvre;

3° les instructions et les conditions strictes dans le cadre desquelles l'infraction peut être commise;

4° les droits et les obligations de la source dans le cadre de la commission de l'infraction autorisée;

Une copie du mémorandum est transmise à la Commission.

§ 5. Dès que l'infraction a été commise et que la source humaine est en sécurité pour le faire, celle-ci fait rapport à l'agent chargé du suivi du déroulement de l'infraction. Ce dernier en informe par écrit le dirigeant du service qui, à son tour, informe par écrit la Commission dans les plus brefs délais.

Si la mesure a été autorisée pour une période supérieure à deux semaines, le service de renseignement et de sécurité concerné fait rapport toutes les deux semaines par écrit à la Commission sur le déroulement de la mesure.

À la demande motivée de la Commission, le rapport est transmis à plus courte échéance, pour autant que l'agent et la source soient en sécurité pour le faire.

§ 6. En cas d'extrême urgence, lorsque des circonstances exceptionnelles et une menace potentielle grave le justifient, le dirigeant du service demande l'accord verbal préalable du président de la Commission ou, s'il n'est pas joignable, d'un autre membre. L'auteur de l'accord en informe immédiatement les autres membres. Le dirigeant du service confirme sa demande par écrit dans les vingt-quatre heures suivant la communication de l'accord. Cette confirmation écrite comprend les mentions visées au paragraphe 2, alinéa 5. Le président ou le membre contacté confirme également son accord par écrit le plus rapidement possible. Cet accord est valable cinq jours. Les conditions préalables prévues aux paragraphes 2 à 4 sont applicables au présent paragraphe.

§ 7. Si la Commission ne rend pas sa décision conformément aux paragraphes 2 ou 6, le dirigeant du service concerné peut saisir le Comité permanent R qui autorisera ou n'autorisera pas la commission de(s) (l')infraction(s) dans les plus brefs délais.

Het memorandum wordt gedateerd en omvat onder meer de volgende vermeldingen:

1° de identificatiecode van de menselijke bron;

2° de wijze waarop het strafbaar feit ten uitvoer zal worden gelegd;

3° de instructies en de strikte voorwaarden in het kader waarvan het strafbaar feit gepleegd mag worden;

4° de rechten en plichten van de bron in het kader van het plegen van het toegelaten strafbaar feit;

Een afschrift van het memorandum wordt overgemaakt aan de Commissie.

§ 5. Zodra het strafbaar feit gepleegd is en de menselijke bron in veiligheid is, brengt deze verslag uit aan de agent belast met de opvolging van het verloop van het strafbaar feit. Deze laatste informeert schriftelijk het diensthoofd dat, op zijn beurt, zo spoedig mogelijk de Commissie schriftelijk informeert.

Indien de maatregel werd toegestaan voor een periode langer dan twee weken, brengt de betrokken inlichtingen- en veiligheidsdienst om de twee weken schriftelijk verslag uit aan de Commissie over het verloop van de maatregel.

Op gemotiveerd verzoek van de Commissie wordt het verslag op een kortere termijn overgemaakt, voor zover de agent en de bron in veiligheid zijn.

§ 6. In geval van hoogdringendheid, wanneer uitzonderlijke omstandigheden en een ernstige potentiële dreiging dit rechtvaardigen, vraagt het diensthoofd het voorafgaand mondeling akkoord van de voorzitter van de Commissie of, indien hij niet bereikbaar is, van een ander lid. Diegene die het akkoord gegeven heeft, brengt de andere leden hier onmiddellijk van op de hoogte. Het diensthoofd bevestigt zijn vraag schriftelijk binnen de vierentwintig uur na mededeling van het akkoord. Deze schriftelijke bevestiging bevat de vermeldingen bedoeld in paragraaf 2, lid 5. De voorzitter of het gecontacteerde lid bevestigt eveneens zo snel mogelijk schriftelijk zijn akkoord. Dit akkoord geldt voor vijf dagen. De voorafgaandelijke voorwaarden bepaald in de paragrafen 2 tot 4 zijn van toepassing op deze paragraaf.

§ 7. Indien de Commissie nalaat haar beslissing uit te brengen overeenkomstig de paragrafen 2 of 6, kan het betrokken diensthoofd het Vast Comité I vatten, dat zo spoedig mogelijk al dan niet de toestemming zal geven om het strafbaar feit of de strafbare feiten te plegen.

En cas de décision négative de la Commission en application des paragraphes 2 ou 6, le dirigeant du service concerné peut saisir le Comité permanent R. Le Comité permanent R autorisera ou n'autorisera pas la commission d'infraction(s) dans les plus brefs délais.

Le Comité permanent R communique sa décision au dirigeant du service et à la Commission.

§ 8. La Commission transmet sans délai tous les documents visés aux paragraphes 2 à 5 au Comité permanent R.

§ 9. Le dirigeant du service met fin à la mesure dès que possible, lorsque l'absolue nécessité de commettre une infraction a disparu, lorsque la mesure n'est plus utile pour la finalité pour laquelle elle avait été demandée ou lorsqu'il a été constaté une illégalité. Il en informe dès que possible la Commission.

Lorsque la Commission ou le Comité permanent R constate une illégalité, elle ou il en informe le dirigeant du service concerné qui met fin à la mesure en cours ou planifiée dès que possible. Ce dernier confirme ensuite par écrit à la Commission et au Comité permanent R que la mesure a pris fin.

§ 10. Les membres de la Commission peuvent contrôler à tout moment la légalité des mesures.

Ils peuvent, à cet effet, avoir accès à la version papier des documents en relation avec la commission d'infraction(s) par la source et entendre l'agent chargé du suivi du déroulement de l'infraction, en présence de son supérieur hiérarchique et de tout autre responsable de la gestion de ladite source.".

Art. 8

Dans le Chapitre III, Section 2, Sous-section 1, insérée par l'article 5, il est inséré un article 13/1/2, rédigé comme suit:

"Art. 13/1/2. § 1er. Lors de l'application des articles 13/1 et 13/1/1, la Commission fonctionne selon les modalités déterminées à l'article 43/1.

§ 2. Sont exemptés de peine, les membres de la Commission qui autorisent la commission des infractions visées aux articles 13/1 et 13/1/1.

In geval van een negatieve beslissing van de Commissie overeenkomstig de paragrafen 2 of 6, kan het betrokken diensthoofd het Vast Comité I vatten. Het Vast Comité I zal zo spoedig mogelijk al dan niet de toestemming geven om het strafbaar feit of de strafbare feiten te plegen.

Het Vast Comité I deelt zijn beslissing mee aan het diensthoofd en aan de Commissie.

§ 8. De Commissie maakt alle documenten bedoeld in de paragrafen 2 tot 5 onverwijld over aan het Vast Comité I.

§ 9. Het diensthoofd beëindigt de maatregel zo snel mogelijk, wanneer de absolute noodzaak om een strafbaar feit te plegen weggevallen is, wanneer de maatregel niet langer nuttig is voor het doel waarvoor hij werd aangevraagd of wanneer een onwettigheid is vastgesteld. Hij brengt zijn beslissing zo snel mogelijk ter kennis van de Commissie.

Indien de Commissie of het Vast Comité I een onwettigheid vaststelt, brengt zij of hij het betrokken diensthoofd hiervan op de hoogte, dat de geplande of lopende maatregel zo snel mogelijk beëindigt. Deze laatste bevestigt vervolgens schriftelijk aan de Commissie en aan het Vast Comité I dat de maatregel beëindigd is.

§ 10. De leden van de Commissie kunnen op elk ogenblik een controle uitoefenen op de wettigheid van de maatregelen.

Zij kunnen daartoe toegang hebben tot de papieren versie van de documenten met betrekking tot het plegen van een strafbaar feit of strafbare feiten door de bron en de agent horen die belast is met de opvolging van het verloop van het strafbaar feit, in het bijzijn van zijn hiërarchische meerdere, en ieder ander die verantwoordelijk is voor de behandeling van voornoemde bron.".

Art. 8

In Hoofdstuk III, Afdeling 2, Onderafdeling 1, ingevoegd bij artikel 5, wordt een artikel 13/1/2 ingevoegd, luidende:

"Art. 13/1/2. § 1. In de toepassing van de artikelen 13/1 en 13/1/1, treedt de Commissie op volgens de modaliteiten bepaald in artikel 43/1.

§ 2. Blijven vrij van straf, de leden van de Commissie die een akkoord verlenen tot het plegen van strafbare feiten zoals bedoeld in de artikelen 13/1 en 13/1/1.

§ 3. Sont exemptés de peine, les membres et les collaborateurs du Comité permanent R, lorsqu'ils exercent leur contrôle dans le cadre de l'application de la présente sous-section.

§ 4. Sont exemptés de peine, les agents des services de renseignement et de sécurité qui encadrent ou contrôlent les agents visés à l'article 13/1 et les sources humaines visées à l'article 13/1/1."

Art. 9

Dans le Chapitre III, Section 2, il est inséré une sous-section 2, rédigée comme suit: "Sous-section 2. Faux nom, fausse qualité, identité fictive et qualité fictive". Cette sous-section comprend l'article 13/2.

Art. 10

Dans la Sous-section 2, insérée par l'article 9, à l'article 13/2, inséré par la loi du 30 mars 2017, les modifications suivantes sont apportées:

1° dans l'alinéa 1er, les mots "nom qui ne lui appartient pas, ainsi qu'une qualité et une identité fictives" sont remplacés par les mots "faux nom, une fausse qualité, une identité fictive ou une qualité fictive";

2° dans la version néerlandaise de l'alinéa 1er, les mots "*te bepalen*" sont remplacés par le mot "*bepaalde*";

3° dans l'alinéa 3, les mots "temporaire et" sont abrogés;

4° dans l'alinéa 4, les mots "d'une fausse qualité," sont insérés entre les mots "d'un faux nom," et les mots "d'une identité et d'une qualité fictives" et le mot "et" entre les mots "d'une identité" et les mots "d'une qualité fictives" est remplacé par le mot "ou";

5° dans la version néerlandaise de l'alinéa 4, le mot "of" entre les mots "*van een valse naam*" et "*van een fictieve identiteit*" est supprimé.

Art. 11

Dans le Chapitre III, Section 2, il est inséré une sous-section 3, rédigée comme suit: "Sous-section 3. La création et l'utilisation de personnes morales". Cette sous-section comprend l'article 13/3.

§ 3. Blijven vrij van straf, de raadsleden en de medewerkers van het Vast Comité I wanneer zij hun toezicht uitoefenen binnen de toepassing van deze onderafdeling.

§ 4. Blijven vrij van straf, de agenten van de inlichtingen- en veiligheidsdiensten die de agenten bedoeld in artikel 13/1 en de menselijke bronnen bedoeld in artikel 13/1/1, begeleiden of controleren."

Art. 9

In Hoofdstuk III, Afdeling 2, wordt een onderafdeling 2 ingevoegd, luidende: "Onderafdeling 2. Valse naam, valse hoedanigheid, fictieve identiteit en fictieve hoedanigheid". Deze onderafdeling bevat artikel 13/2.

Art. 10

In Onderafdeling 2, ingevoegd bij artikel 9, worden in artikel 13/2, ingevoegd bij de wet van 30 maart 2017, de volgende wijzigingen aangebracht:

1° in het eerste lid worden de woorden "een naam die hem niet toebehoort alsook van een fictieve identiteit en hoedanigheid" vervangen door de woorden "een valse naam, een valse hoedanigheid, een fictieve identiteit of een fictieve hoedanigheid";

2° in het eerste lid worden in de Nederlandse versie de woorden "te bepalen" vervangen door het woord "bepaalde";

3° in het derde lid worden de woorden "tijdelijk en" opgeheven;

4° in het vierde lid worden de woorden ", van een valse hoedanigheid," ingevoegd tussen de woorden "van een valse naam" en de woorden "of van een fictieve identiteit en hoedanigheid" en wordt het woord "en" tussen de woorden "fictieve identiteit" en het woord "hoedanigheid" vervangen door het woord "of";

5° in de Nederlandstalige versie van het vierde lid wordt het woord "of" tussen de woorden "van een valse naam" en de woorden "van een fictieve identiteit" geschrapt.

Art. 11

In Hoofdstuk III, Afdeling 2, wordt een onderafdeling 3 ingevoegd, luidende: "Onderafdeling 3. De oprichting en inzet van rechtspersonen". Deze onderafdeling bevat artikel 13/3.

Art. 12

Dans le Chapitre III, Section 2, il est inséré une sous-section 4, rédigée comme suit: “Sous-section 4. Le concours de tiers”. Cette sous-section comprend l’article 13/4.

Art. 13

Dans la Sous-section 4, insérée par l’article 12, à l’article 13/4, inséré par la loi du 30 mars 2017, les modifications suivantes sont apportées:

1° L’alinéa 3 est remplacé par ce qui suit:

“Les paragraphes 2 à 6 et 8 à 9 de l’article 13/1 et le paragraphe 11 de l’article 13/1/1 sont applicables aux tiers qui fournissent directement une aide ou une assistance nécessaire pour l’application de la présente loi.”;

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

“L’aide et l’assistance apportées se font toujours sous le contrôle du service de renseignement et de sécurité concerné, qui garde la direction de l’opération.”.

Art. 14

À l’article 16/3 de la même loi, inséré par la loi du 25 décembre 2016, les modifications suivantes sont apportées:

1° au paragraphe 2, alinéa 1er, les mots “ou son délégué” sont insérés entre les mots “le dirigeant du service” et les mots “et communiquée”;

2° au paragraphe 2, un alinéa rédigé comme suit est inséré entre les alinéas 1 et 2:

“En cas d’urgence, le dirigeant du service ou son délégué peut décider verbalement d’accéder à ces données. Cette décision verbale est confirmée par une décision écrite, le premier jour ouvrable qui suit la date de la décision, selon les modalités fixées à l’alinéa 1er.”;

3° au paragraphe 2, alinéa 2, devenu alinéa 3, dans la version française, les mots “dans les conditions qui ne respectent pas les conditions légales” sont remplacés par les mots “dans des conditions qui ne respectent pas les dispositions légales” et dans la version néerlandaise, le mot “*voorwaarden*” est remplacé par le mot “*bepalingen*”.

Art. 12

In Hoofdstuk III, Afdeling 2, wordt een onderafdeling 4 ingevoegd, luidende: “Onderafdeling 4. De medewerking van derden”. Deze onderafdeling bevat artikel 13/4.

Art. 13

In Onderafdeling 4, ingevoegd bij artikel 12, worden in artikel 13/4, ingevoegd bij de wet van 30 maart 2017, de volgende wijzigingen aangebracht:

1° Het derde lid wordt vervangen als volgt:

“De paragrafen 2 tot 6 en 8 tot 9 van artikel 13/1 en paragraaf 11 van artikel 13/1/1 zijn van toepassing op de derden die noodzakelijke en rechtstreekse hulp en bijstand verlenen voor de toepassing van deze wet.”;

2° het artikel wordt aangevuld met een lid, luidende:

“De verleende hulp en bijstand geschiedt te allen tijde onder het toezicht van de betrokken inlichtingen- en veiligheidsdienst, die de leiding behoudt over de operatie.”.

Art. 14

In artikel 16/3 van dezelfde wet, ingevoegd bij de wet van 25 december 2016, worden de volgende wijzigingen aangebracht:

1° in paragraaf 2, eerste lid, worden de woorden “een diensthoofd” vervangen door de woorden “het diensthoofd of zijn gedelegeerde”;

2° in paragraaf 2 wordt tussen het eerste en het tweede lid een lid ingevoegd, luidende:

“In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde mondeling beslissen om toegang te hebben tot deze gegevens. Deze mondelinge beslissing wordt de eerste werkdag volgend op de datum van de beslissing bevestigd door een schriftelijke beslissing, volgens de nadere regels bepaald in het eerste lid.”;

3° in paragraaf 2, tweede lid, dat het derde lid is geworden, worden in de Franstalige versie de woorden “*dans les conditions qui ne respectent pas les conditions légales*” vervangen door de woorden “*dans des conditions qui ne respectent pas les dispositions légales*” en wordt in de Nederlandstalige versie het woord “voorwaarden” vervangen door het woord “bepalingen”.

Art. 15

À l'article 16/4 de la même loi, inséré par la loi du 21 mars 2018, les modifications suivantes sont apportées:

1° au paragraphe 2, 1er alinéa , le mot "artikels" est remplacé par les mots "de artikelen" dans la version néerlandaise, et les mots "officier de renseignement" sont remplacés par les mots "officier des méthodes";

2° au paragraphe 2, un alinéa est inséré entre les alinéas 2 et 3, rédigé comme suit:

"En cas d'urgence, le dirigeant du service ou son délégué peut décider verbalement d'accéder à ces données. Cette décision verbale est confirmée par une décision écrite, le premier jour ouvrable qui suit la date de la décision, selon les modalités fixées à l'alinéa 4.";

3° au paragraphe 2, alinéa 3, devenu alinéa 4, dans la version française, les mots "les conditions qui ne respectent pas les conditions légales" sont remplacés, par les mots "des conditions qui ne respectent pas les dispositions légales" et dans la version néerlandaise, le mot "*voorwaarden*" est remplacé par le mot "*bepalingen*";

4° au paragraphe 3, alinéa 2, les mots "d'un officier de renseignement" sont remplacés par les mots "d'un officier des méthodes";

5° au paragraphe 3, alinéa 3, dans la version française, les mots "les circonstances qui ne respectent pas les conditions légales" sont remplacés par les mots "des conditions qui ne respectent pas les dispositions légales" et dans la version néerlandaise, le mot "voorwaarden" est remplacé par le mot "bepalingen";

6° au paragraphe 5, alinéa 2, le mot "enquête" est remplacé par le mot "information".

7° au paragraphe 6, les mots "L'officier de renseignement" sont remplacés par les mots "L'officier des méthodes".

Art. 16

Dans le Chapitre III, Section 4, Sous-section 1re, il est inséré un article 16/5, rédigé comme suit:

Art. 15

In artikel 16/4 van dezelfde wet, ingevoegd bij de wet van 21 maart 2018, worden de volgende wijzigingen aangebracht:

1° in paragraaf 2, eerste lid, wordt het woord "artikels" vervangen door de woorden "de artikelen" in de Nederlandstalige versie en worden de woorden "een inlichtingenofficier" vervangen door de woorden "een methodenofficier";

2° in paragraaf 2 wordt tussen het tweede en het derde lid een lid ingevoegd, luidende:

"In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde mondeling beslissen om toegang te hebben tot deze gegevens. Deze mondelinge beslissing wordt de eerste werkdag volgend op de datum van de beslissing bevestigd door een schriftelijke beslissing volgens de nadere regels bepaald in het vierde lid.";

3° in paragraaf 2, derde lid, dat het vierde lid is geworden, worden in de Franstalige versie de woorden "les conditions qui ne respectent pas les conditions légales" vervangen door de woorden "des conditions qui ne respectent pas les dispositions légales" en in de Nederlandstalige versie wordt het woord "voorwaarden" vervangen door het woord "bepalingen"

4° in paragraaf 3, tweede lid, worden de woorden "een inlichtingenofficier" vervangen door de woorden "een methodenofficier";

5° in paragraaf 3, derde lid, worden in de Franstalige versie de woorden "les circonstances qui ne respectent pas les conditions légales" vervangen door de woorden "des conditions qui ne respectent pas les dispositions légales" en wordt in de Nederlandstalige versie het woord "voorwaarden" vervangen door het woord "bepalingen";

6° in paragraaf 5, tweede lid, worden de woorden "opsporingsonderzoek of gerechtelijk onderzoek" vervangen door de woorden "opsporings- of gerechtelijk onderzoek";

7° in paragraaf 6 worden de woorden "De inlichtingenofficier" vervangen door de woorden "De methodenofficier".

Art. 16

In Hoofdstuk III, Afdeling 4, Onderafdeling 1, wordt een artikel 16/5 ingevoegd, luidende:

"Art. 16/5. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, s'infiltrer dans le monde virtuel, sous couvert ou non d'un faux nom ou d'une fausse qualité.".

Art. 17

Dans le Chapitre III, Section 4, Sous-section 1re, il est inséré un article 16/6 rédigé comme suit:

"Art. 16/6. § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours:

1° des personnes et institutions visées à l'article 5, paragraphe 1er, 3° à 22°, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces;

2° des personnes et institutions qui, sur le territoire belge, mettent à disposition ou proposent des services en lien avec des valeurs virtuelles permettant d'échanger des moyens de paiement réglementés en valeurs virtuelles;

3° du Point de Contact Central tenu par la Banque nationale de Belgique conformément à la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt;

afin de procéder à:

a) l'identification des produits et services dont la personne visée est le titulaire, le mandataire ou le bénéficiaire effectif;

b) l'identification des titulaires, des mandataires ou des bénéficiaires effectifs des produits et services.

Le dirigeant du service ou son délégué effectue la réquisition, visée à l'alinéa 1er, 1° et 2°, par écrit. En cas d'extrême urgence, le dirigeant du service ou son délégué peut requérir ces données verbalement. Cette réquisition verbale doit être confirmée par écrit dans un délai de vingt-quatre heures.

La coopération requise visée à l'alinéa 1er, , 3 ° a lieu après une décision écrite du dirigeant du service ou de son délégué, et conformément à la loi du 8 juillet 2018 portant organisation d'un point de contact central

"Art. 16/5. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, in de virtuele wereld infiltreren, al dan niet onder dekmantel van een valse naam of valse hoedanigheid.".

Art. 17

In Hoofdstuk III, Afdeling 4, Onderafdeling 1, wordt een artikel 16/6 ingevoegd, luidende:

"Art. 16/6. § 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van:

1° de personen en instellingen bedoeld in artikel 5, paragraaf 1, 3° tot 22° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;

2° de personen en instellingen die, binnen het Belgisch grondgebied, diensten beschikbaar stellen of aanbieden met betrekking tot virtuele waarden die toelaten dat gereglementeerde betaalmiddelen in virtuele waarden worden uitgewisseld;

3° het Centraal Aanspreekpunt gehouden door de Nationale Bank van België overeenkomstig de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van bankrekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest;

om over te gaan tot:

a) het identificeren van de producten en diensten, waarvan de geviseerde persoon titularis, gevolmachtigde of de uiteindelijke gerechtigde is;

b) het identificeren van de titularissen, de gevolmachtigden, of de uiteindelijke gerechtigden van de producten en diensten.

De vordering bedoeld in het eerste lid, 1° en 2° gebeurt schriftelijk door het diensthoofd of zijn gedelegeerde. In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde deze gegevens mondeling vorderen. Deze mondelinge vordering wordt binnen de vierentwintig uur bevestigd door een schriftelijke vordering.

De gevorderde medewerking bedoeld in het eerste lid, 3° gebeurt na schriftelijke beslissing van het diensthoofd of zijn gedelegeerde, en overeenkomstig de wet van 8 juli 2018 houdende organisatie van een

des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt. En cas d'extrême urgence, le dirigeant du service ou son délégué peut autoriser verbalement la méthode. Cette décision verbale est confirmée par une décision écrite dans un délai de vingt-quatre heures.

§ 2. La personne ou l'institution requise est tenue de remettre sans délai les informations demandées après réception de la réquisition écrite du dirigeant du service ou de son délégué.

La personne ou l'institution requise qui refuse de prêter le concours visé au présent article est punie d'une amende de vingt-six euros à vingt mille euros.

§ 3. Les deux services de renseignement et de sécurité tiennent un registre de toutes les identifications requises. Le service de renseignement et de sécurité concerné transmet chaque mois au Comité permanent R une liste des identifications requises.

Le Comité permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans des conditions qui ne respectent pas les dispositions légales.".

Art. 18

À l'article 18 de la même loi, inséré par la loi du 4 février 2010 et modifié en dernier lieu par la loi du 30 mars 2017, les modifications suivantes sont apportées:

1° l'actuel alinéa 1er formera le paragraphe 1er;

2° à l'alinéa 1er, devenu le paragraphe 1er, les mots "à des personnes dont" sont insérés entre les mots "avoir recours" et les mots "des sources humaines";

3° il est inséré un paragraphe 2, rédigé comme suit:

"§ 2. Dans l'intérêt de l'exercice de leurs missions visées aux articles 7, 1° et 3°/1 et 11, § 1er, 1° à 3° et 5°, les services de renseignement et de sécurité peuvent mettre en œuvre des méthodes de recueil de données à l'égard d'une source humaine:

1° lorsqu'il y a un doute quant à sa fiabilité, discrétion ou loyauté vis-à-vis du service de renseignement et de

centraal aanspreekpunt van bankrekeningen en financiele contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest. In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde de methode mondeling toestaan. Deze mondelinge beslissing wordt binnen de vierentwintig uur bevestigd door een schriftelijke beslissing.

§ 2. De gevorderde persoon of instelling is ertoe gehouden de gevraagde informatie onverwijld te verstrekken na ontvangst van de schriftelijke vordering van het diensthoofd of zijn gedelegeerde.

De gevorderde persoon of instelling die de in dit artikel bedoelde medewerking weigert te verlenen, wordt gestraft met geldboete van zesentwintig euro tot twintigduizend euro.

§ 3. Beide inlichtingen- en veiligheidsdiensten houden een register bij van alle gevorderde identificaties. De betrokken inlichtingen- en veiligheidsdienst maakt maandelijks een lijst van de gevorderde identificaties over aan het Vast Comité I.

Het Vast Comité I verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke bepalingen voldoen.".

Art. 18

In artikel 18 van dezelfde wet, ingevoegd bij de wet van 4 februari 2010 en laatstelijk gewijzigd bij de wet van 30 maart 2017, worden de volgende wijzigingen aangebracht:

1° de bestaande tekst van het eerste lid zal paragraaf 1 vormen;

2° in het huidige eerste lid, waarvan de tekst paragraaf 1 zal worden, worden de woorden "op personen waaronder" ingevoegd tussen de woorden "een beroep doen" en de woorden "menselijke bronnen";

3° er wordt een paragraaf 2 ingevoegd, luidende:

"§ 2. In het belang van de uitvoering van hun opdrachten bedoeld in de artikelen 7, 1° en 3°/1 en 11, § 1, 1° tot 3° en 5°, kunnen de inlichtingen- en veiligheidsdiensten de methoden voor het verzamelen van gegevens aanwenden ten opzichte van een menselijke bron:

1° indien er twijfel bestaat over zijn betrouwbaarheid, discretie of loyauteit tegenover de betrokken

sécurité concerné susceptible de causer un préjudice pour l'exercice des missions dudit service, ou

2° pour assurer sa protection.".

Art. 19

L'article 18/1 de la même loi, inséré par la loi du 4 février 2010 et modifié en dernier lieu par la loi du 30 mars 2017, est complété par le 3° rédigé comme suit:

"3° sans préjudice des 1° et 2°, aux services de renseignement et de sécurité, dans le cadre de l'article 18, paragraphe 2.".

Art. 20

À l'article 18/2 de la même loi, inséré par la loi du 4 février 2010 et modifié par la loi du 30 mars 2017, les modifications suivantes sont apportées:

1° au paragraphe 3, alinéa 1er, première phrase, les signes de paragraphe "§§" sont remplacés par le mot "paragraphes".

2° au paragraphe 3, alinéa 1er, première phrase, les mots "visée à l'article 3, 6°" sont remplacés par les mots "ou, en cas d'empêchement, par un autre membre de la Commission";

3° au paragraphe 3, alinéa 1er, deuxième phrase, les mots "ou le membre de la Commission qui remplace le président" sont insérés entre les mots "Le président de la commission" et les mots "est tenu de fournir";

4° au paragraphe 3, alinéa 2 , les signes de paragraphe "§§" sont remplacés par le mot "paragraphes".

5° au paragraphe 3, alinéa 2, les mots "ou, en cas d'empêchement, un autre membre de la Commission" sont insérés entre les mots "le président de la commission" et les mots "vérifie si les données";

6° au paragraphe 3, alinéa 3, le signe de paragraphe "§" est remplacé par le mot "paragraphe".

7° L'article est complété par un paragraphe 4, rédigé comme suit:

"§ 4. Lorsqu'une méthode visée aux paragraphes 1er et 2 est mise en œuvre à l'égard d'une source humaine

inlichtingen- en veiligheidsdienst waardoor een nadeel ontstaat voor de uitoefening van de opdrachten van die dienst, of

2° ter verzekering van zijn bescherming.".

Art. 19

Artikel 18/1 van dezelfde wet, ingevoegd bij de wet van 4 februari 2010 en laatstelijk gewijzigd bij de wet van 30 maart 2017, wordt aangevuld met de bepaling onder 3°, luidende:

"3° onverminderd 1° en 2°, op de inlichtingen- en veiligheidsdiensten, in het kader van artikel 18, paragraaf 2.".

Art. 20

In artikel 18/2 van dezelfde wet, ingevoegd bij de wet van 4 februari 2010 en gewijzigd bij de wet van 30 maart 2017, worden de volgende wijzigingen aangebracht:

1° in paragraaf 3, eerste lid, eerste zin, worden de paragraaftekens "§§" vervangen door het woord "paragrafen".

2° in paragraaf 3, eerste lid, eerste zin, worden de woorden "bedoeld in artikel 3, 6°" vervangen door de woorden "of, bij verhindering, door een ander Commissielid";

3° in paragraaf 3, eerste lid, tweede zin, worden de woorden "of het Commissielid dat de voorzitter vervangt," ingevoegd tussen de woorden "De voorzitter van de commissie" en de woorden "is verplicht om";

4° in paragraaf 3, tweede lid, worden de paragraaftekens "§§" vervangen door het woord "paragrafen".

5° in paragraaf 3, tweede lid, worden de woorden "of, bij verhindering, een ander Commissielid," ingevoegd tussen de woorden "de voorzitter van de commissie" en de woorden "na of de via deze methode";

6° in paragraaf 3, derde lid, wordt het paragraafteken "§" vervangen door het woord "paragraaf".

7° het artikel wordt aangevuld met een paragraaf 4, luidende:

"§ 4. Indien een in de paragrafen 1 en 2 bedoelde methode wordt aangewend ten opzichte van een menselijke

en application de l'article 18, § 2, il est dérogé aux mentions prescrites sous peine de nullité prévues aux articles 18/3, § 2, 2° et 3° et 18/10, § 2, 2° et 3°.".

Art. 21

À l'article 18/3 de la même loi, inséré par la loi du 4 février 2010 et modifié en dernier lieu par la loi du 30 mars 2017, les modifications suivantes sont apportées:

1° au paragraphe 1er, alinéa 1er, première phrase, les mots "ou dans le cadre de l'article 18, § 2," sont insérés entre les mots "la menace potentielle visée à l'article 18/1" et les mots "si les méthodes ordinaires";

2° Le paragraphe 1er, alinéa 1er est complété par les mots "ou en fonction du degré de gravité du préjudice potentiel pour l'exercice des missions des services ou du danger potentiel pour la sécurité de la source humaine dans le cadre de l'article 18, § 2.";

3° au paragraphe 2, 6°, les mots "du (ou des) officier(s) de renseignement" sont remplacés par les mots "du (ou des) officier(s) des méthodes";

4° au paragraphe 2, 9°, les mots "les infractions" sont remplacés par les mots "les faits susceptibles d'être qualifiés infraction(s)";

5° le paragraphe 2 est complété par un alinéa rédigé comme suit:

"Dans le cadre de l'article 18 § 2 et par dérogation au paragraphe 2, 2° et 3°, la décision du dirigeant du service mentionne respectivement le code d'identification de la source humaine et le préjudice potentiel pour l'exercice des missions des services ou le danger potentiel pour la sécurité de la source humaine.";

6° au paragraphe 3, alinéa 2, les mots "l'officier de renseignement" sont à chaque fois remplacés par les mots "l'officier des méthodes", et le numéro d'article "18/6/1," est inséré entre les numéros "18/6," et "18/7";

7° au paragraphe 6, alinéa 1er, les mots "mesures, y compris le respect des principes de subsidiarité et de proportionnalité" sont remplacés par les mots "méthodes spécifiques de recueil de données, y compris le respect des principes de subsidiarité et de proportionnalité prévu à l'article 18/3, § 1er";

bron in toepassing van artikel 18, § 2, wordt van de op straffe van nietigheid voorgeschreven vermeldingen bepaald in de artikelen 18/3, § 2, 2° en 3° en 18/10, § 2, 2° en 3° afgeweken.".

Art. 21

In artikel 18/3 van dezelfde wet, ingevoegd bij de wet van 4 februari 2010 en laatstelijk gewijzigd bij de wet van 30 maart 2017, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, eerste lid, eerste zin, worden de woorden "of in het kader van artikel 18, § 2," ingevoegd tussen de woorden "een potentiële dreiging zoals bedoeld in artikel 18/1" en de woorden "kunnen de in artikel";

2° paragraaf 1, eerste lid, wordt aangevuld met de woorden "of in functie van de graad van ernst van het potentieel nadeel voor de uitoefening van de opdrachten van de diensten of het potentiële gevaar voor de veiligheid van de menselijke bron in het kader van artikel 18, § 2.";

3° in paragraaf 2, 6°, worden de woorden "van de inlichtingenofficier(en)" vervangen door de woorden "van de methodenofficier(en)";

4° in paragraaf 2, 9°, worden de woorden "de strafbare feiten" vervangen door de woorden "de feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd";

5° paragraaf 2 wordt aangevuld met een lid, luidende:

"In het kader van artikel 18, § 2 en in afwijking van paragraaf 2, 2° en 3°, vermeldt de beslissing van het diensthoofd respectievelijk de identificatiecode van de menselijke bron en het potentieel nadeel voor de uitoefening van de opdrachten van de diensten of het potentiële gevaar voor de veiligheid van de menselijke bron.";

6° in paragraaf 3, tweede lid, worden de woorden "De inlichtingenofficier" telkens vervangen door de woorden "De methodenofficier" en wordt het artikelnummer "18/6/1," ingevoegd tussen de nummers "18/6," en "18/7";

7° in paragraaf 6, eerste lid, worden de woorden "maatregelen, hierbij inbegrepen de naleving van de principes van subsidiariteit en proportionaliteit" vervangen door de woorden "specifieke methoden voor het verzamelen van gegevens, hierbij inbegrepen de naleving van de principes van subsidiariteit en proportionaliteit bepaald in artikel 18/3, § 1";

8° au paragraphe 6, alinéa 3, les mots “de la commission de la protection de la vie privée” sont remplacés par les mots “du Comité permanent R”;

9° au paragraphe 7, les mots “L’officier de renseignement“ sont remplacés par les mots “L’officier des méthodes”.

Art. 22

Dans la même loi, un article 18/5/1 est inséré, libellé comme suit:

“Art. 18/5/1. Les services de renseignement et de sécurité peuvent, dans l’intérêt de l’exercice de leurs missions, s’infiltrer dans le monde virtuel sous couvert d’une identifié fictive ou d’une qualité fictive.”

Art. 23

À l’article 18/9 de la même loi, inséré par la loi du 4 février 2010 et modifié en dernier lieu par la loi du 30 mars 2017, les modifications suivantes sont apportées:

1° au paragraphe 1er, le 1° est complété par les mots “ou dans le cadre de l’article 18, § 2 lorsqu’il existe un préjudice potentiel grave pour l’exercice des missions des services ou un danger potentiel grave pour la sécurité de la source humaine”;

2° au paragraphe 1er, le 2° est complété par les mots “ou, dans le cadre de l’article 18, § 2 lorsqu’il existe un préjudice potentiel grave pour l’exercice des missions des services ou un danger potentiel grave pour la sécurité de la source humaine”;

3° au paragraphe 2, alinéa 1er, les mots “compte tenu d’une menace potentielle visée au paragraphe 1er” sont remplacés par les mots “compte tenu d’une menace, d’un préjudice ou d’un danger potentiel visé au paragraphe 1er”;

4° le paragraphe 3 est complété par les mots “ou en fonction du degré de gravité du préjudice potentiel pour l’exercice des missions des services ou du danger potentiel pour la sécurité de la source humaine dans le cadre de l’article 18 § 2.”.

8° in paragraaf 6, derde lid, worden de woorden “de commissie voor de bescherming van de persoonlijke levenssfeer” vervangen door de woorden “het Vast Comité I”;

9° in paragraaf 7 worden de woorden “De inlichtingenofficier” vervangen door de woorden “De methodenofficier”.

Art. 22

In dezelfde wet wordt een artikel 18/5/1 ingevoegd, luidende:

“Art. 18/5/1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, in de virtuele wereld infiltreren onder dekmantel van een fictieve identiteit of fictieve hoedanigheid.”

Art. 23

In artikel 18/9 van dezelfde wet, ingevoegd bij de wet van 4 februari 2010 en laatstelijk gewijzigd bij de wet van 30 maart 2017, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 wordt de bepaling onder 1° aangevuld met de woorden “of in het kader van artikel 18, § 2, indien er ernstig potentieel nadeel bestaat voor de uitoefening van de opdrachten van de diensten of een ernstig potentieel gevaar voor de veiligheid van de menselijke bron”;

2° in paragraaf 1 wordt de bepaling onder 2° aangevuld met de woorden “of in het kader van artikel 18, § 2, indien er een ernstig potentieel nadeel bestaat voor de uitoefening van de opdrachten van de diensten of een ernstig potentieel gevaar voor de veiligheid van de menselijke bron”;

3° in paragraaf 2, eerste lid, worden de woorden “rekening houdend met een potentiële dreiging zoals bedoeld in artikel 18/1” vervangen door de woorden “rekening houdend met een potentiële dreiging, nadeel of gevaar zoals bedoeld in paragraaf 1”;

4° paragraaf 3 wordt aangevuld met de woorden “of in functie van de graad van de ernst van het potentieel nadeel voor de uitoefening van de opdrachten van de diensten of het potentiële gevaar voor de veiligheid van de menselijke bron in het kader van artikel 18 § 2.”.

Art. 24

À l'article 18/10 de la même loi, inséré par la loi du 4 février 2010 et modifié par la loi du 30 mars 2017, les modifications suivantes sont apportées:

1° au paragraphe 1er, alinéa 3, les mots "L'officier de renseignement" sont remplacés par les mots "L'officier des méthodes";

2° au paragraphe 2, 6° les mots "des officier(s) de renseignement" sont remplacés par les mots "des officier(s) des méthodes";

3° au paragraphe 2, 9°, les mots "les infractions" sont remplacés par les mots "les faits susceptibles d'être qualifiés infraction(s)";

4° le paragraphe 2 est complété par un alinéa rédigé comme suit:

"Dans le cadre de l'article 18 § 2 et par dérogation au paragraphe 2, 2° et 3°, la décision du dirigeant du service mentionne respectivement le code d'identification de la source humaine et le préjudice potentiel grave pour l'exercice des missions des services ou le danger potentiel grave pour la sécurité de la source humaine.";

5° au paragraphe 4, alinéa 4, les mots "L'officier de renseignement" sont remplacés par les mots "L'officier des méthodes";

6° au paragraphe 4, alinéas 8 et 9, les mots "Si le président" sont remplacés par les mots "Si le président ou le membre de la Commission contacté";

7° dans le paragraphe 6, alinéa 4, les mots "de la commission de la protection de la vie privée" sont remplacés par les mots "du Comité permanent R".

Art. 25

Dans la même loi, un article 18/12/1 est inséré, libellé comme suit:

"Art. 18/12/1. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, s'infiltrer dans le monde réel, conformément aux directives du Conseil national de sécurité.

Art. 24

In artikel 18/10 van dezelfde wet, ingevoegd bij de wet van 4 februari 2010 en gewijzigd bij de wet van 30 maart 2017, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1, derde lid, worden de woorden "De inlichtingenofficier" vervangen door de woorden "De methodenofficier";

2° in paragraaf 2, 6°, worden de woorden "van de inlichtingenofficier(en)" vervangen door de woorden "van de methodenofficier(en)";

3° in paragraaf 2, 9°, worden de woorden "de strafbare feiten" vervangen door de woorden "de feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd";

4° paragraaf 2 wordt aangevuld met een lid, luidende:

"In het kader van artikel 18 § 2 en in afwijking van paragraaf 2, 2° en 3°, vermeldt de beslissing van het diensthoofd respectievelijk de identificatiecode van de menselijke bron en het potentieel nadeel voor de uitoefening van de opdrachten van de diensten of het potentiële gevaar voor de veiligheid van de menselijke bron.";

5° in paragraaf 4, vierde lid, worden de woorden "De inlichtingenofficier" vervangen door de woorden "De methodenofficier";

6° in paragraaf 4, achtste en negende lid, worden de woorden "Indien de voorzitter" vervangen door de woorden "Indien de voorzitter of het gecontacteerde Commissielid";

7° in paragraaf 6, vierde lid, worden de woorden "de commissie voor de bescherming van de persoonlijke levenssfeer" vervangen door de woorden "het Vast Comité I".

Art. 25

In dezelfde wet wordt een artikel 18/12/1 ingevoegd, luidende:

"Art. 18/12/1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, in de reële wereld infiltreren, conform de richtlijnen van de Nationale Veiligheidsraad.

Le monde réel vise les relations qui se déroulent principalement avec des contacts physiques directs sans dissimuler son apparence physique.

La méthode est autorisée aussi longtemps qu'elle est nécessaire aux finalités pour lesquelles elle est mise en œuvre.

Le service de renseignement et de sécurité concerné fait rapport à la Commission tous les deux mois sur l'évolution de la menace qui a nécessité le recours à l'infiltration dans le monde réel. Ce rapport met en évidence les éléments qui justifient soit le maintien de la méthode exceptionnelle, soit la fin de celle-ci.".

Art. 26

L'article 18/15 de la même loi, inséré par la loi du 4 février 2010 et modifié par la loi du 30 mars 2017, est remplacé par ce qui suit:

"Art. 18/15. § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir des informations relatives aux produits, services et transactions de nature financière et aux valeurs virtuelles, concernant la personne visée, auprès:

1° des personnes et institutions visées à l'article 5, paragraphe 1er, 3° à 22° de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces;

2° des personnes et institutions qui, sur le territoire belge, mettent à disposition ou proposent des services en lien avec des valeurs virtuelles permettant d'échanger des moyens de paiement réglementés en valeurs virtuelles;

3° du Point de Contact Central tenu par la Banque nationale de Belgique conformément à la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt.

§ 2. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, exiger des personnes et institutions visées au paragraphe 1er, 1° et 2° le placement sous surveillance des transactions de la personne visée.

Met reële wereld wordt bedoeld de relaties die hoofdzakelijk plaatsvinden via rechtstreekse fysieke contacten zonder dat daarbij zijn fysieke uiterlijk verborgen wordt.

De methode is toegelaten zolang als nodig is voor het doel waarvoor ze wordt aangewend.

De betrokken inlichtingen- en veiligheidsdienst brengt om de twee maanden verslag uit aan de Commissie over de evolutie van de dreiging die het beroep op een infiltratie in de reële wereld noodzakelijk maakte. Dit verslag benadrukt de elementen die hetzij het behoud, hetzij de stopzetting van de uitzonderlijke methode rechtvaardigen.".

Art. 26

Artikel 18/15 van dezelfde wet, ingevoegd bij de wet van 4 februari 2010 en gewijzigd bij de wet van 30 maart 2017, wordt vervangen als volgt:

"Art. 18/15. § 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, informatie over de producten, diensten en verrichtingen van financiële aard en betreffende virtuele valuta, met betrekking tot de geviseerde persoon vorderen van:

1° de personen en instellingen bedoeld in artikel 5, paragraaf 1, 3° tot 22° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;

2° de personen en instellingen die, binnen het Belgisch grondgebied, diensten beschikbaar stellen of aanbieden met betrekking tot virtuele waarden die toelaten dat gereglementeerde betaalmiddelen in virtuele waarden worden uitgewisseld;

3° het Centraal Aanspreekpunt gehouden door de Nationale Bank van België overeenkomstig de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van bankrekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest.

§ 2. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, van de personen en instellingen bedoeld in paragraaf 1, 1° en 2° vorderen dat de verrichtingen van de geviseerde persoon onder toezicht worden geplaatst.

§ 3. La coopération requise visée au paragraphe 1er, 3° a lieu conformément à la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt.

La personne ou l'institution requise, visée au paragraphe 1er, 1° et 2°, est tenue de remettre sans délai les informations demandées après réception de la réquisition écrite du dirigeant du service.

Cette réquisition mentionne, selon le cas, la nature de l'avis conforme de la Commission, la nature de l'avis conforme du président de la Commission ou la nature de l'autorisation du ministre concerné. Dans la réquisition, le service de renseignement et de sécurité concerné fournit également une description précise des informations requises et détermine la forme sous laquelle elles doivent être communiquées.

§ 4. Toute personne ou institution requise qui refuse de communiquer les données ou qui ne les communique pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition est punie d'un emprisonnement de huit jours à un an et d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement.".

Art. 27

À l'article 20 de la même loi, les modifications suivantes sont apportées:

1° dans la version française du paragraphe 1er, le mot "collaboration" est remplacé par le mot "coopération";

2° au paragraphe 2, les mots ", dans les limites d'un protocole approuvé par les ministres concernés," sont supprimés";

§ 3. De gevorderde medewerking bedoeld in paragraaf 1, 3° gebeurt overeenkomstig de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van bankrekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest.

De gevorderde persoon of instelling, bedoeld in paragraaf 1, 1° en 2°, is ertoe gehouden de gevraagde informatie onverwijld te verstrekken na ontvangst van de schriftelijke vordering van het diensthoofd.

Deze vordering vermeldt, naargelang het geval, de aard van het eensluidend advies van de Commissie, de aard van het eensluidend advies van de voorzitter van de Commissie of de aard van de toelating van de betrokken minister. In deze vordering beschrijft de betrokken inlichtingen- en veiligheidsdienst eveneens nauwkeurig de informatie die wordt gevorderd en de vorm waarin deze wordt meegedeeld.

§ 4. Iedere gevorderde persoon of instelling die de gegevens weigert mee te delen of niet meedeelt in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, wordt gestraft met gevangenisstraf van acht dagen tot een jaar en met geldboete van zesentwintig euro tot twintigduizend euro of met een van die straffen alleen.".

Art. 27

In artikel 20 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° in de Franstalige versie van paragraaf 1 wordt het woord *"collaboration"* vervangen door het woord *"coopération"*;

2° in paragraaf 2 worden de woorden "binnen de perken van een protocol goedgekeurd door de betrokken ministers ," verwijderd";

3° le paragraphe 2 est complété par un alinéa libellé comme suit:

"Les modalités de ce concours peuvent être déterminées dans le cadre d'un protocole.".

Donné à Bruxelles le 30 Mai 2022

PHILIPPE

PAR LE ROI:

Le ministre de la Justice,

Vincent Van Quickenborne

La ministre de la Défense,

Ludivine DEDONDER

3° paragraaf 2 wordt aangevuld met een lid, luidende:

"De nadere regels voor deze medewerking kunnen in het kader van een protocol worden vastgelegd.".

Gegeven te Brussel op 30 mei 2022

FILIP

VAN KONINGSWEGE:

De minister van Justitie,

Vincent Van Quickenborne

De minister van Defensie,

Ludivine DEDONDER

COORDINATION DES ARTICLES

TEXTE DE BASE	TEXTE DE BASE ADAPTÉ AU PROJET
Art. 3.	**Art. 3.**
La présente loi entend par :	La présente loi entend par :
1° "Conseil national de sécurité": le Conseil créé au sein du Gouvernement, qui est chargé des tâches de sécurité nationale déterminées par le Roi;	1° "Conseil national de sécurité" : le Conseil créé au sein du Gouvernement, qui est chargé des tâches de sécurité nationale déterminées par le Roi ;
2° " agent " : tout membre du personnel statutaire ou contractuel et tout militaire exerçant ses fonctions au sein des services de renseignement et de sécurité visés à l'article 2;	2° " agent " : tout membre du personnel statutaire ou contractuel et tout militaire exerçant ses fonctions au sein des services de renseignement et de sécurité visés à l'article 2;
3° "membre de l'équipe d'intervention":	3° "membre de l'équipe d'intervention" :
a) pour la Sûreté de l'Etat, l'agent visé aux articles 22 à 35 chargé de la protection du personnel, des infrastructures et des biens de la Sûreté de l'Etat;	a) pour la Sûreté de l'Etat, l'agent visé aux articles 22 à 35 chargé de la protection du personnel, des infrastructures et des biens de la Sûreté de l'Etat;
b) pour le Service Général du Renseignement et de la Sécurité, l'agent visé aux articles 22 à 35 chargé de la protection du personnel, des infrastructures et des biens du Service Général du Renseignement et de la Sécurité;	b) pour le Service Général du Renseignement et de la Sécurité des Forces armées, l'agent visé aux articles 22 à 35 chargé de la protection du personnel, des infrastructures et des biens du Service Général du Renseignement et de la Sécurité ;
4° " Service Général du Renseignement et de la Sécurité " : le Service Général du Renseignement et de la Sécurité.	4° " Service Général du Renseignement et de la Sécurité " : le Service Général du Renseignement et de la Sécurité **des Forces armées** ;
5° " le Ministre " : le Ministre de la Justice en ce qui concerne la Sûreté de l'Etat, et le Ministre de la Défense en ce qui concerne le [4 Service Général du Renseignement et de la Sécurité;	5° " le Ministre " : le Ministre de la Justice en ce qui concerne la Sûreté de l'Etat, et le Ministre de la Défense en ce qui concerne le Service Général du Renseignement et de la Sécurité ;

6° " la commission " : la commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données des services de renseignement et de sécurité, créée par l'article 43/1;	6° " la ~~c~~ **C**ommission " : la commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données des services de renseignement et de sécurité, créée par l'article 43/1;
7° " le Comité permanent R " : le Comité permanent de contrôle des services de renseignement visé dans la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements et de l'Organe de coordination pour l'analyse de la menace;	7° " le Comité permanent R " : le Comité permanent de contrôle des services de renseignement visé dans la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements et de l'Organe de coordination pour l'analyse de la menace;
8° " le dirigeant du service " : d'une part, l'administrateur général de la Sûreté de l'Etat ou, en cas d'empêchement, l'administrateur général faisant fonction et, d'autre part, le chef du Service Général du Renseignement et de la Sécurité ou, en cas d'empêchement, le chef faisant fonction;	8° " le dirigeant du service " : d'une part, l'administrateur général de la Sûreté de l'Etat ou, en cas d'empêchement, l'administrateur général faisant fonction et, d'autre part, le chef du Service Général du Renseignement et de la Sécurité ou, en cas d'empêchement, le chef faisant fonction;
	8°/1 « son délégué »: l'agent, autre que le gestionnaire du dossier, désigné par décision écrite du dirigeant du service transmise au Comité permanent R, pour prendre habituellement certaines décisions à la place du dirigeant du service ;
9° " l'officier de renseignement " :	9° " l'officier **des méthodes** ~~de renseignement~~ " :
a) pour la Sûreté de l'Etat, l'agent revêtu au moins du grade de commissaire;	a) pour la Sûreté de l'Etat, l'agent revêtu au moins du grade de commissaire;
b) pour le Service Général du Renseignement et de la Sécurité, l'officier affecté à ce service, ainsi que l'agent civil revêtu au moins du grade de commissaire;	b) pour le Service Général du Renseignement et de la Sécurité, l'officier affecté à ce service, ainsi que l'agent civil revêtu au moins du grade de commissaire;
10° " communications " : toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de données de toute nature, par fil, radio-électricité,	10° " communications " : toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de données de toute nature, par fil, radio-électricité, signalisation

signalisation optique ou un autre système électromagnétique; les communications par téléphone, GSM, mobilophone, télex, télécopieur ou la transmission électronique de données par ordinateur ou réseau informatique, ainsi que toute autre communication privée;	optique ou un autre système électromagnétique; les communications par téléphone, GSM, mobilophone, télex, télécopieur ou la transmission électronique de données par ordinateur ou réseau informatique, ainsi que toute autre communication privée;
11° " réseaux de communications électroniques " : les réseaux de communications électroniques visés à l'article 2, 3°, de la loi du 13 juin 2005 relative aux communications électroniques;	11° " réseaux de communications électroniques " : les réseaux de communications électroniques visés à l'article 2, 3°, de la loi du 13 juin 2005 relative aux communications électroniques;
11° /1 "fournisseur d'un service de communications électroniques": quiconque qui, de quelque manière que ce soit, met à disposition ou offre, sur le territoire belge, un service qui consiste en la transmission de signaux via des réseaux de communications électroniques ou qui permet aux utilisateurs, via un réseau de communications électroniques, d'obtenir, de recevoir ou de diffuser des informations;	11° /1 "fournisseur d'un service de communications électroniques": quiconque qui, de quelque manière que ce soit, met à disposition ou offre, sur le territoire belge, un service qui consiste en la transmission de signaux via des réseaux de communications électroniques ou qui permet aux utilisateurs, via un réseau de communications électroniques, d'obtenir, de recevoir ou de diffuser des informations;
12° "lieu accessible au public": tout lieu, public ou privé, auquel le public peut avoir accès;	12° "lieu accessible au public": tout lieu, public ou privé, auquel le public peut avoir accès;
12° /1 "lieu non accessible au public non soustrait à la vue": tout lieu auquel le public n'a pas accès et qui est visible de tous à partir de la voie publique sans moyen ou artifice, à l'exception de l'intérieur des bâtiments non accessibles au public;	12° /1 "lieu non accessible au public non soustrait à la vue": tout lieu auquel le public n'a pas accès et qui est visible de tous à partir de la voie publique sans moyen ou artifice, à l'exception de l'intérieur des bâtiments non accessibles au public;
13° " courrier " : l'envoi postal tel qu'il est défini à l'article 131, 6°, 7° et 11°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques;	13° " courrier " : l'envoi postal tel qu'il est défini à l'article 131, 6°, 7° et 11°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques;
14° " moyen technique " : une configuration de composants qui détecte des signaux, les transmet, active leur enregistrement et enregistre les signaux, à l'exception d':	14° " moyen technique " : une configuration de composants qui détecte des signaux, les transmet, active leur enregistrement et enregistre les signaux, à l'exception d':

a) un appareil utilisé pour la prise de photographies;	a) un appareil utilisé pour la prise de photographies;
b) un appareil mobile utilisé pour la prise d'images animées lorsque la prise de photographies ne permet pas de garantir la discrétion et la sécurité des agents et à la condition que cette utilisation ait été préalablement autorisée par le dirigeant du service ou son délégué. Seules les images fixes jugées pertinentes sont conservées. Les autres images sont détruites dans le mois qui suit le jour de l'enregistrement;	b) un appareil mobile utilisé pour la prise d'images animées lorsque la prise de photographies ne permet pas de garantir la discrétion et la sécurité des agents et à la condition que cette utilisation ait été préalablement autorisée par le dirigeant du service ou son délégué. Seules les images fixes jugées pertinentes sont conservées. Les autres images sont détruites dans le mois qui suit le jour de l'enregistrement;
15° " processus de radicalisation " : un processus influençant un individu ou un groupe d'individus de telle sorte que cet individu ou ce groupe d'individus soit mentalement préparé ou disposé à commettre des actes terroristes;	15° " processus de radicalisation " : un processus influençant un individu ou un groupe d'individus de telle sorte que cet individu ou ce groupe d'individus soit mentalement préparé ou disposé à commettre des actes terroristes;
16° " journaliste " : le journaliste admis à porter le titre de journaliste professionnel conformément à la loi du 30 décembre 1963 relative à la reconnaissance et à la protection du titre de journaliste professionnel;	16° " journaliste " : le journaliste admis à porter le titre de journaliste professionnel conformément à la loi du 30 décembre 1963 relative à la reconnaissance et à la protection du titre de journaliste professionnel;
17° " secret des sources " : le secret tel qu'il est défini dans la loi du 7 avril 2005 relative à la protection des sources journalistes;	17° " secret des sources " : le secret tel qu'il est défini dans la loi du 7 avril 2005 relative à la protection des sources journalistes;
18° " Directeur des Opérations de la Sûreté de l'Etat " : l'agent des services extérieurs de la Sûreté de l'Etat revêtu du grade de commissaire général qui est chargé de la direction des services extérieurs de la Sûreté de l'Etat;	18° " Directeur des Opérations de la Sûreté de l'Etat " : l'agent des services extérieurs de la Sûreté de l'Etat revêtu du grade de commissaire général qui est chargé de la direction des services extérieurs de la Sûreté de l'Etat;
19° "objet verrouillé": un objet dont l'ouverture nécessite une fausse clé ou une effraction;	19° "objet verrouillé": un objet dont l'ouverture nécessite une fausse clé ou une effraction;
20° "observation": la surveillance d'une ou de plusieurs personnes, de leur présence ou de	20° "observation": la surveillance d'une ou de plusieurs personnes, de leur présence ou de leur comportement, de choses, lieux ou événements;

leur comportement, de choses, lieux ou événements;	
21° "inspection": la pénétration, l'examen et la fouille d'un lieu ainsi que l'examen et la fouille d'un objet.	21° "inspection": la pénétration, l'examen et la fouille d'un lieu ainsi que l'examen et la fouille d'un objet.
	22° « faux nom » : un nom qui n'appartient pas à l'agent et qui n'est pas attesté par une carte d'identité, un passeport, une carte d'étranger ou un document de séjour ou par des documents officiels en découlant ;
	23° « fausse qualité » : une qualité qui n'appartient pas à l'agent et dont il ne découle aucun effet juridique ;
	24° « identité fictive » : une fausse identité attestée par une carte d'identité, un passeport, une carte d'étranger ou un document de séjour ;
	25° « qualité fictive » : un statut, un titre ou une fonction n'appartenant pas à l'agent dont il découle des effets juridiques ;
	26° « source humaine » : une personne qui donne une information aux services de renseignement et de sécurité et qui est enregistrée conformément à la procédure prévue dans la directive portant sur le recours à des sources humaines approuvées par le Conseil national de sécurité ;
	27° « s'infiltrer » : le fait pour un agent, en dehors des cas visés à l'article 18, de s'intégrer délibérément dans un groupe ou dans la vie d'une personne afin de recueillir des informations ou des données, dans le cadre d'une enquête d'un service de renseignement et de sécurité et dans l'intérêt de l'exercice de ses missions, soit dans le monde virtuel, soit dans le monde réel. Cet agent dissimule sa qualité d'agent des services de renseignement et de sécurité et, pour les agents

	du Service Général du Renseignement et de la Sécurité, de membre du Ministère de la Défense, et :
	a) participe ou facilite les activités ou soutient activement les convictions ou les activités de la personne ou du groupe qui fait l'objet de l'enquête, ou
	b) entretient des relations durables avec ceux-ci.
Art. 11.	**Art. 11.**
§ 1er. Le Service Général du Renseignement et de la Sécurité a pour mission:	§ 1er. Le Service Général du Renseignement et de la Sécurité a pour mission:
1° de rechercher, d'analyser et de traiter le renseignement relatif aux facteurs qui influencent ou peuvent influencer la sécurité nationale et internationale dans la mesure où les Forces armées sont ou pourraient être impliquées, en fournissant un soutien en renseignement à leurs opérations en cours ou à leurs éventuelles opérations à venir, ainsi que le renseignement relatif à toute activité qui menace ou pourrait menacer:	1° de rechercher, d'analyser et de traiter le renseignement relatif aux facteurs qui influencent ou peuvent influencer la sécurité nationale et internationale dans la mesure où les Forces armées sont ou pourraient être impliquées, en fournissant un soutien en renseignement à leurs opérations en cours ou à leurs éventuelles opérations à venir, ainsi que le renseignement relatif à toute activité qui menace ou pourrait menacer:
a) l'intégrité du territoire national ou la population,	a) l'intégrité du territoire national ou la population,
b) les plans de défense militaires,	b) les plans de défense militaires,
c) le potentiel scientifique et économique en rapport avec les acteurs, tant personnes physiques que personnes morales, qui sont actifs dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Conseil national de sécurité, sur proposition du ministre de la Justice et du ministre de la Défense,	c) le potentiel scientifique et économique en rapport avec les acteurs, tant personnes physiques que personnes morales, qui sont actifs dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Conseil national de sécurité, sur proposition du ministre de la Justice et du ministre de la Défense,

d) l'accomplissement des missions des Forces armées,	d) l'accomplissement des missions des Forces armées,
e) la sécurité des ressortissants belges à l'étranger,	e) la sécurité des ressortissants belges à l'étranger,
f) tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité;	f) tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité;
et d'en informer sans délai les ministres compétents ainsi que de donner des avis au gouvernement, à la demande de celui-ci, concernant la définition de sa politique intérieure et étrangère de sécurité et de défense;	et d'en informer sans délai les ministres compétents ainsi que de donner des avis au gouvernement, à la demande de celui-ci, concernant la définition de sa politique intérieure et étrangère de sécurité et de défense;
2° de veiller au maintien de la sécurité militaire du personnel relevant du Ministre de la Défense nationale, et des installations militaires, armes et systèmes d'armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires et, dans le cadre des cyberattaques de systèmes d'armes, de systèmes informatiques et de communications militaires ou de ceux que le Ministre de la Défense nationale gère, de neutraliser l'attaque et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit des conflits armés;	2° de veiller au maintien de la sécurité militaire du personnel relevant du Ministre de la Défense nationale, et des installations militaires, armes et systèmes d'armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires et, dans le cadre des cyberattaques de systèmes d'armes, de systèmes informatiques et de communications militaires ou de ceux que le Ministre de la Défense nationale gère, de neutraliser l'attaque et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit **international** ~~des conflits armés~~;
	2°/1 de neutraliser, dans le cadre d'une crise nationale de cybersécurité, une cyberattaque de systèmes informatiques et de communications non gérés par le Ministre de la Défense et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit international ;
3° de protéger le secret qui, en vertu des engagements internationaux de la Belgique ou afin d'assurer l'intégrité du territoire national	3° de protéger le secret qui, en vertu des engagements internationaux de la Belgique ou afin d'assurer l'intégrité du territoire national et

et l'accomplissement des missions des Forces armées, s'attache aux installations militaires, armes, munitions, équipements, aux plans, écrits, documents ou autres objets militaires, aux renseignements et communications militaires, ainsi qu'aux systèmes informatiques et de communications militaires ou ceux que le Ministre de la Défense nationale gère;	l'accomplissement des missions des Forces armées, s'attache aux installations militaires, armes, munitions, équipements, aux plans, écrits, documents ou autres objets militaires, aux renseignements et communications militaires, ainsi qu'aux systèmes informatiques et de communications militaires ou ceux que le Ministre de la Défense nationale gère;
4° d'effectuer les enquêtes de sécurité qui lui sont confiées conformément aux directives du Conseil national de sécurité.	4° d'effectuer les enquêtes de sécurité qui lui sont confiées conformément aux directives du Conseil national de sécurité ;~~.~~
5° de rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge.	5° de rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge ;~~.~~
	6° d'exécuter toutes autres missions qui lui sont confiées par ou en vertu de la loi.
§ 2. Pour l'application du § 1er, on entend par :	§ 2. Pour l'application du § 1er, on entend par :
1° " activité qui menace ou pourrait menacer l'intégrité du territoire national ou la population " : toute manifestation de l'intention de, par des moyens de nature militaire, saisir, occuper ou agresser tout ou partie du territoire national, de l'espace aérien au-dessus de ce territoire ou de la mer territoriale, ou porter atteinte à la protection ou à la survie de tout ou partie de la population, au patrimoine national ou au potentiel économique du pays;	1° " activité qui menace ou pourrait menacer l'intégrité du territoire national ou la population " : toute manifestation de l'intention de, par des moyens de nature militaire, saisir, occuper ou agresser tout ou partie du territoire national, de l'espace aérien au-dessus de ce territoire ou de la mer territoriale, ou porter atteinte à la protection ou à la survie de tout ou partie de la population, au patrimoine national ou au potentiel économique du pays;
2° " activité qui menace ou pourrait menacer les plans de défense militaires " : toute manifestation de l'intention de prendre connaissance par voie illicite des plans relatifs à la défense militaire du territoire national, de l'espace aérien au-dessus de ce territoire ou de la mer territoriale et des intérêts vitaux de l'Etat, ou à la défense militaire commune dans le cadre d'une alliance ou d'une collaboration internationale ou supranationale;	2° " activité qui menace ou pourrait menacer les plans de défense militaires " : toute manifestation de l'intention de prendre connaissance par voie illicite des plans relatifs à la défense militaire du territoire national, de l'espace aérien au-dessus de ce territoire ou de la mer territoriale et des intérêts vitaux de l'Etat, ou à la défense militaire commune dans le cadre d'une alliance ou d'une collaboration internationale ou supranationale;

2°/1 " activité qui menace ou pourrait menacer le potentiel scientifique et économique en rapport avec les acteurs, tant personnes physiques que personnes morales, qui sont actifs dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Conseil national de sécurité, sur proposition du Ministre de la Justice et du Ministre de la Défense " : toute manifestation de l'intention de porter atteinte aux éléments essentiels du potentiel scientifique et économique de ces acteurs;	2°/1 " activité qui menace ou pourrait menacer le potentiel scientifique et économique en rapport avec les acteurs, tant personnes physiques que personnes morales, qui sont actifs dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Conseil national de sécurité, sur proposition du Ministre de la Justice et du Ministre de la Défense " : toute manifestation de l'intention de porter atteinte aux éléments essentiels du potentiel scientifique et économique de ces acteurs;
3° " activité qui menace ou pourrait menacer l'accomplissement des missions des Forces armées " : toute manifestation de l'intention de neutraliser, d'entraver, de saboter, de porter atteinte ou d'empêcher la mise en condition, la mobilisation et la mise en œuvre des Forces armées belges, des Forces armées alliées ou des organismes de défense interalliés lors de missions, actions ou opérations dans le cadre national, dans le cadre d'une alliance ou d'une collaboration internationale ou supranationale;	3° " activité qui menace ou pourrait menacer l'accomplissement des missions des Forces armées " : toute manifestation de l'intention de neutraliser, d'entraver, de saboter, de porter atteinte ou d'empêcher la mise en condition, la mobilisation et la mise en œuvre des Forces armées belges, des Forces armées alliées ou des organismes de défense interalliés lors de missions, actions ou opérations dans le cadre national, dans le cadre d'une alliance ou d'une collaboration internationale ou supranationale;
4° " activité qui menace ou pourrait menacer la sécurité des ressortissants belges à l'étranger " : toute manifestation de l'intention de porter collectivement atteinte à la vie ou à l'intégrité physique de ressortissants belges à l'étranger et des membres de leur famille.	4° " activité qui menace ou pourrait menacer la sécurité des ressortissants belges à l'étranger " : toute manifestation de l'intention de porter collectivement atteinte à la vie ou à l'intégrité physique de ressortissants belges à l'étranger et des membres de leur famille.
	5° « crise nationale de cybersécurité » : tout incident de cybersécurité qui, par sa nature ou ses conséquences :
	– **menace les intérêts vitaux du pays ou les besoins essentiels de la population ;**
	– **requiert des décisions urgentes ; et**

	– **demande une action coordonnée de plusieurs départements et organismes.**
§ 3. A la requête du Service Général du Renseignement et de la Sécurité, la Sûreté de l'Etat prête son concours pour recueillir le renseignement lorsque des personnes qui ne relèvent pas du Ministre de la Défense nationale ou qui ne relèvent pas d'entreprises qui exécutent des contrats conclus avec lui, avec des organisations militaires internationales ou avec des pays tiers en matière militaire, ou qui participent à une procédure de passation de marché public lancée par ceux-ci, sont impliquées dans les activités visées au paragraphe 1er, 1°, 2°, 3°, et 5°.	§ 3. A la requête du Service Général du Renseignement et de la Sécurité, la Sûreté de l'Etat prête son concours pour recueillir le renseignement lorsque des personnes qui ne relèvent pas du Ministre de la Défense nationale ou qui ne relèvent pas d'entreprises qui exécutent des contrats conclus avec lui, avec des organisations militaires internationales ou avec des pays tiers en matière militaire, ou qui participent à une procédure de passation de marché public lancée par ceux-ci, sont impliquées dans les activités visées au paragraphe 1er, 1°~~, 2°,~~ **à** 3°**,** ~~et~~ 5° **et 6°**.
Les mesures de protection industrielle ne seront prises qu'à la demande du Ministre de la Défense nationale, de pays tiers ou des organisations avec lesquelles la Belgique est liée par traité, convention ou contrat.	Les mesures de protection industrielle ne seront prises qu'à la demande du Ministre de la Défense nationale, de pays tiers ou des organisations avec lesquelles la Belgique est liée par traité, convention ou contrat.
Art. 13.	**Art. 13.**
Les services de renseignement et de sécurité peuvent rechercher, collecter, recevoir et traiter des informations et des données à caractère personnel qui peuvent être utiles à l'exécution de leurs missions et tenir à jour une documentation relative notamment à des événements, à des groupements et à des personnes présentant un intérêt pour l'exécution de leurs missions.	**§1er.** Les services de renseignement et de sécurité peuvent rechercher, collecter, recevoir et traiter des informations et des données à caractère personnel qui peuvent être utiles à l'exécution de leurs missions et tenir à jour une documentation relative notamment à des événements, à des groupements et à des personnes présentant un intérêt pour l'exécution de leurs missions.
Les renseignements contenus dans la documentation doivent présenter un lien avec la finalité du fichier et se limiter aux exigences qui en découlent.	Les renseignements contenus dans la documentation doivent présenter un lien avec la finalité du fichier et se limiter aux exigences qui en découlent.
Les services de renseignement et de sécurité veillent à la sécurité des données ayant trait à leurs sources et à celles des informations et des données à caractère personnel fournies par ces sources.	**§2.** Les services de renseignement et de sécurité veillent à la sécurité des données ayant trait à leurs sources et à celles des informations et des données à caractère personnel fournies par ces sources.

Les agents des services de renseignement et de sécurité ont accès aux informations, renseignements et données à caractère personnel recueillis et traités par leur service, pour autant que ceux-ci soient utiles dans l'exercice de leur fonction ou de leur mission.	**§3.** Les agents des services de renseignement et de sécurité ont accès aux informations, renseignements et données à caractère personnel recueillis et traités par leur service, pour autant que ceux-ci soient utiles dans l'exercice de leur fonction ou de leur mission.
	§4. Lorsque, au cours d'une enquête ou d'une vérification de sécurité au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, un agent prend connaissance d'informations indiquant l'existence d'une menace potentielle visée aux article 7 et 8 ou contre un intérêt visé à l'article 11, il les transmet immédiatement par écrit au dirigeant de son service, ou à son délégué, en vue de leur traitement pour lutter contre ladite menace.
	Sous-section 1 – Commission d'infractions
Art. 13/1.	**Art. 13/1.**
Il est interdit aux agents de commettre des infractions.	**§1er**. Il est interdit aux agents de commettre des infractions.
	§2. Par dérogation au paragraphe 1er, sont exemptés de peine les agents qui commettent des contraventions, des infractions au code de la route ou un vol d'usage, qui sont absolument nécessaires afin d'assurer l'exécution optimale de la mission ou de garantir leur propre sécurité ou celle de tiers, lorsque ces agents sont :
	1° chargés d'exécuter les méthodes de recueil de données ; ou
	2° membres de l'équipe d'intervention.
Par dérogation à l'alinéa 1er, sont exemptés de peine les agents chargés d'exécuter les méthodes de recueil de données, ainsi que les	~~Par dérogation à l'alinéa, sont exemptés de peine les agents chargés d'exécuter les méthodes de recueil de données, ainsi que les membres de~~

membres de l'équipe d'intervention dans le cadre de leur fonction, qui commettent des contraventions, des infractions au code de la route ou un vol d'usage, qui sont absolument nécessaires afin d'assurer l'exécution optimale de la méthode ou de garantir leur propre sécurité ou celle d'autres personnes.	~~l'équipe d'intervention dans le cadre de leur fonction, qui commettent des contraventions, des infractions au code de la route ou un vol d'usage, qui sont absolument nécessaires afin d'assurer l'exécution optimale de la méthode ou de garantir leur propre sécurité ou celle~~ d'autres ~~personnes~~.
Sans préjudice de l'alinéa 2, sont exemptés de peine, les agents qui, lors de l'exécution des méthodes visées à l'article 18/2, commettent, avec l'accord écrit préalable de la Commission rendu dans les quatre jours de la réception de la demande écrite du dirigeant du service des infractions absolument nécessaires afin d'assurer l'exécution optimale de la méthode ou de garantir leur propre sécurité ou celle d'autres personnes. En cas d'extrême urgence, le dirigeant du service demande l'accord verbal préalable du président de la Commission. Cet accord verbal est confirmé par écrit, le plus rapidement possible, par le président de la Commission. La Commission ou le président notifie son accord au Comité permanent R.	~~Sans préjudice de l'alinéa 2, sont exemptés de peine, les agents qui, lors de l'exécution des méthodes visées à l'article 18/2, commettent, avec l'accord écrit préalable de la Commission rendu dans les quatre jours de la réception de la demande écrite du dirigeant du service des infractions absolument nécessaires afin d'assurer l'exécution optimale de la méthode ou de garantir leur propre sécurité ou celle d'autres personnes. En cas d'extrême urgence, le dirigeant du service demande l'accord verbal préalable du président de la Commission. Cet accord verbal est confirmé par écrit, le plus rapidement possible, par le président de la Commission. La Commission ou le président notifie son accord au Comité permanent R.~~
Par dérogation à l'alinéa 3, s'il n'a pas été possible de prévoir l'absolue nécessité de commettre une infraction pour garantir la sécurité des agents ou celle d'autres personnes et d'obtenir l'accord préalable de la Commission ou du président en cas de procédure d'extrême urgence, le dirigeant du service informe celle-ci dans les plus brefs délais qu'une infraction a été commise. Si après évaluation, la Commission conclut à l'absolue nécessité et à l'imprévisibilité de l'infraction, l'agent est exempté de peine. La Commission transmet cet accord au Comité permanent R.	~~Par dérogation à l'alinéa 3, s'il n'a pas été possible de prévoir l'absolue nécessité de commettre une infraction pour garantir la sécurité des agents ou celle d'autres personnes et d'obtenir l'accord préalable de la Commission ou du président en cas de procédure d'extrême urgence, le dirigeant du service informe celle-ci dans les plus brefs délais qu'une infraction a été commise. Si après évaluation, la Commission conclut à l'absolue nécessité et à l'imprévisibilité de l'infraction, l'agent est exempté de peine. La Commission transmet cet accord au Comité permanent R.~~
Les infractions visées aux alinéas 2 à 4 doivent être directement proportionnelles à l'objectif visé par la mission de renseignement et ne peuvent en aucun cas porter atteinte à l'intégrité physique des personnes.	~~Les infractions visées aux alinéas 2 à 4 doivent être directement proportionnelles à l'objectif visé par la mission de renseignement et ne peuvent en aucun cas porter atteinte à l'intégrité physique des personnes.~~

Les membres de la commission qui autorisent à commettre des infractions visées aux alinéas 3 et 4 n'encourent aucune peine.	~~Les membres de la commission qui autorisent à commettre des infractions visées aux alinéas 3 et 4 n'encourent aucune peine.~~
	§3. Sans préjudice du paragraphe 2, sont exemptés de peine, les agents qui, lors de l'exécution des missions visées aux articles 7, 1° et 3°/1 et 11, §1er, 1° à 3° et 5°, commettent des infractions absolument nécessaires afin d'assurer l'exécution optimale de leur mission ou de garantir leur propre sécurité ou celle de tiers.
	Les infractions visées à l'alinéa 1er ne peuvent être commises qu'avec l'accord écrit préalable de la Commission. La Commission donne son accord écrit dans les quatre jours suivant la réception de la demande écrite et motivée du dirigeant du service.
	L'accord ne peut porter sur une période supérieure à six mois, sans préjudice de la possibilité de prolonger la mesure en suivant la procédure visée à l'alinéa 2.
	La demande du dirigeant du service mentionne, sous peine d'illégalité :
	1° les faits susceptibles d'être qualifiés infraction(s);
	2° le contexte de la demande et la finalité;
	3° la liste des agents répondant au profil requis pour commettre les faits susceptibles d'être qualifiés infraction(s) visés au 1° ;
	4° l'absolue nécessité;
	5° la proportionnalité visée au paragraphe 4;

	6° la période durant laquelle la ou les infractions peuvent être commises à compter de l'accord de la Commission et la motivation de la durée de la période;
	7° le cas échéant, les motifs qui justifient l'extrême urgence visée au paragraphe 6;
	8° le nom du ou des agent(s) chargé(s) du suivi du déroulement de l'infraction ;
	9° la date de la demande;
	10° la signature du dirigeant du service.
	§4. Les infractions doivent être directement proportionnelles à l'objectif visé par la mission et ne peuvent en aucun cas porter atteinte à l'intégrité physique des personnes.
	§5. L'agent qui assure le suivi du déroulement de l'infraction fait rapport par écrit au dirigeant du service le plus rapidement possible après la commission de l'infraction.
	Le service de renseignement et de sécurité concerné en informe la Commission par écrit dans les plus brefs délais.
	Par dérogation à l'alinéa 2, si la mesure a été autorisée pour une période supérieure à deux mois, le service de renseignement et de sécurité concerné informe la Commission du déroulement de la mesure par écrit toutes les deux semaines.
	A la demande motivée de la Commission, le rapport est transmis à plus courte échéance, pour autant que l'agent qui a commis l'infraction soit en sécurité pour le faire.

	§6. En cas d'extrême urgence, le dirigeant du service demande l'accord verbal préalable du président de la Commission ou, s'il n'est pas joignable, d'un autre membre. L'auteur de l'accord en informe immédiatement les autres membres. Le dirigeant du service confirme sa demande par écrit dans les vingt-quatre heures suivant la communication de l'accord. Cette confirmation écrite comprend les mentions visées au paragraphe 3, alinéa 4. Le président ou le membre contacté confirme également son accord par écrit le plus rapidement possible. Cet accord est valable cinq jours.
	§7. Si, en raison de circonstances imprévisibles, les faits susceptibles d'être qualifiés infraction(s) ont été commis pour lesquels la procédure prévue aux paragraphes 3 ou 6 n'a pas pu être suivie, le dirigeant du service en informe la Commission par écrit dans les plus brefs délais et au plus tard dans les vingt-quatre heures qui suivent sa prise de connaissance de la commission des faits susceptibles d'être qualifiés infraction(s). L'agent qui a commis ces faits bénéficie de l'exemption de peine si la Commission estime qu'ils étaient imprévisibles et strictement nécessaires pour assurer sa propre sécurité ou celle de tiers.
	§8. Si la Commission ne rend pas sa décision conformément aux paragraphes 3, 6 ou 7, le dirigeant du service concerné peut saisir le Comité permanent R qui autorisera ou n'autorisera pas la commission de(s) (l') infraction(s) dans les plus brefs délais.
	En cas de décision négative de la Commission en application des paragraphes 3, 6 ou 7, le dirigeant du service concerné peut saisir le Comité permanent R. Le Comité permanent R autorisera ou n'autorisera pas la commission d'infraction(s) dans les plus brefs délais. Le Comité permanent R communique sa décision au dirigeant du service et à la Commission.

	§9. La Commission transmet sans délai tous les documents visés aux paragraphes 3 à 7 au Comité permanent R.
	§10. Le dirigeant du service met fin à la mesure dès que possible lorsque l'absolue nécessité de commettre une infraction a disparu, lorsque la mesure n'est plus utile pour la finalité pour laquelle elle avait été demandée ou lorsqu'il a été constaté une illégalité. Il en informe dès que possible la Commission et le Comité permanent R.
	Lorsque la Commission ou le Comité permanent R constate une illégalité, elle ou il en informe par écrit le dirigeant du service concerné. Ce dernier met fin à la mesure en cours ou planifiée dès que possible et confirme ensuite par écrit à la Commission et au Comité permanent R que la mesure a pris fin.
	§11. Les membres de la Commission peuvent contrôler à tout moment la légalité des mesures.
	Ils peuvent, à cet effet, avoir accès aux données relatives à la mesure, se saisir de toutes les pièces utiles et entendre les membres du service.
	Art. 13/1/1.
	§1. Il est interdit aux sources humaines de commettre des infractions.
	§2. Par dérogation au paragraphe 1er, sont exemptées de peine les sources humaines majeures d'âge qui, dans l'intérêt de l'exercice des missions du service de renseignement et de sécurité concerné, telles que visées aux articles 7, 1° et 3°/1 et 11, §1er, 1°à 3° et 5°, commettent des infractions absolument nécessaires afin d'assurer leur position d'information ou de garantir leur propre sécurité ou celle de tiers.

	Les infractions ne peuvent être commises qu'avec l'accord écrit préalable de la Commission. La Commission donne son accord écrit dans les quatre jours suivant la réception de la demande écrite et motivée du dirigeant du service.
	L'accord ne peut porter sur une période supérieure à deux mois, sans préjudice de la possibilité de prolonger la mesure en suivant la procédure visée à l'alinéa 2.
	Une analyse de risque(s) portant sur la fiabilité de la source et les risques qu'elle encourt dans le cadre de la commission de(s) (l')infraction(s) doit être réalisée préalablement à la demande du dirigeant du service.
	La demande du dirigeant du service mentionne, sous peine d'illégalité :
	1° le code d'identification de la source humaine ;
	2° les faits susceptibles d'être qualifiés infraction(s);
	3° le contexte de la demande et la finalité;
	4° la synthèse de l'analyse de risque(s) visée à l'alinéa 4;
	5° l'absolue nécessité;
	6° la proportionnalité visée au paragraphe 3;
	7° les conditions strictes imposées à la source humaine ;
	8° la période durant laquelle la ou les infractions peuvent être commises et la motivation de la durée de la période;

	9° le cas échéant, les motifs qui justifient l'extrême urgence visée au paragraphe 6;
	10° le nom du ou des agent(s) chargé(s) du suivi du déroulement de l'infraction;
	11° la date de la demande;
	12° la signature du dirigeant du service.
	§3. Les infractions doivent être directement proportionnelles à l'objectif visé par la mission et ne peuvent en aucun cas porter atteinte à l'intégrité physique des personnes.
	§4. Avant que l'infraction autorisée ne puisse être commise, la source humaine signe un mémorandum contenant notamment les modalités de mise en œuvre et de rapportage. Ce mémorandum est conservé dans le dossier individuel de la source humaine.
	Le mémorandum est daté et inclut notamment les mentions suivantes :
	1° le code d'identification de la source humaine ;
	2° la manière dont l'infraction sera mise en œuvre ;
	3° les instructions et les conditions strictes dans le cadre desquelles l'infraction peut être commise ;
	4° les droits et les obligations de la source dans le cadre de la commission de l'infraction autorisée ;

	Une copie du mémorandum est transmise à la Commission.
	§5. Dès que l'infraction a été commise et que la source humaine est en sécurité pour le faire, celle-ci fait rapport à l'agent chargé du suivi du déroulement de l'infraction. Ce dernier en informe par écrit le dirigeant du service qui, à son tour, informe par écrit la Commission dans les plus brefs délais.
	Si la mesure a été autorisée pour une période supérieure à deux semaines, le service de renseignement et de sécurité concerné fait rapport toutes les deux semaines par écrit à la Commission, sur le déroulement de la mesure.
	A la demande motivée de la Commission, le rapport est transmis à plus courte échéance, pour autant que l'agent et la source soient en sécurité pour le faire.
	§6. En cas d'extrême urgence, lorsque des circonstances exceptionnelles et une menace potentielle grave le justifient, le dirigeant du service demande l'accord verbal préalable du président de la Commission ou, s'il n'est pas joignable, d'un autre membre. L'auteur de l'accord en informe immédiatement les autres membres. Le dirigeant du service confirme sa demande par écrit dans les vingt-quatre heures suivant la communication de l'accord. Cette confirmation écrite comprend les mentions visées au paragraphe 2, alinéa 5. Le président ou le membre contacté confirme également son accord par écrit le plus rapidement possible. Cet accord est valable cinq jours. Les conditions préalables prévues aux paragraphes 2 à 4 sont applicables au présent paragraphe.
	§7. Si la Commission ne rend pas sa décision conformément aux paragraphes 2 ou 6, le

	dirigeant du service concerné peut saisir le Comité permanent R qui autorisera ou n'autorisera pas la commission de(s) (l')infraction(s) dans les plus brefs délais.
	En cas de décision négative de la Commission en application des paragraphes 2 ou 6, le dirigeant du service concerné peut saisir le Comité permanent R. Le Comité permanent R autorisera ou n'autorisera pas la commission d'infraction(s) dans les plus brefs délais. **Le Comité permanent R communique sa décision au dirigeant du service et à la Commission.**
	§8. La Commission transmet sans délai tous les documents visés aux paragraphes 2 à 5 au Comité permanent R.
	§9. Le dirigeant du service met fin à la mesure dès que possible, lorsque l'absolue nécessité de commettre une infraction a disparu, lorsque la mesure n'est plus utile pour la finalité pour laquelle elle avait été demandée ou lorsqu'il a été constaté une illégalité. Il en informe dès que possible la Commission.
	Lorsque la Commission ou le Comité permanent R constate une illégalité, elle ou il en informe le dirigeant du service concerné qui met fin à la mesure en cours ou planifiée dès que possible. **Ce dernier confirme ensuite par écrit à la Commission et au Comité permanent R que la mesure a pris fin.**
	§10. Les membres de la Commission peuvent contrôler à tout moment la légalité des mesures.
	Ils peuvent, à cet effet, avoir accès à la version papier des documents en relation avec la commission d'infraction(s) par la source et entendre l'agent chargé du suivi du déroulement de l'infraction, en présence de son supérieur hiérarchique et de tout autre responsable de la gestion de ladite source.

	Art. 13/1/2.
	§1. Lors de l'application des articles 13/1 et 13/1/1, la Commission fonctionne selon les modalités déterminées à l'article 43/1.
	§2. Sont exemptés de peine, les membres de la Commission qui autorisent la commission des infractions visées aux articles 13/1 et 13/1/1.
	§3. Sont exemptés de peine, les membres et les collaborateurs du Comité permanent R, lorsqu'ils exercent leur contrôle dans le cadre de l'application de la présente sous-section.
	§4. Sont exemptés de peine, les agents des services de renseignement et de sécurité qui encadrent ou contrôlent les agents visés à l'article 13/1 et les sources humaines visées à l'article 13/1/1.
	Sous-section 2.- Faux nom, fausse qualité, identité fictive et qualité fictive
Art. 13/2.	**Art. 13/2.**
Un agent peut, pour des raisons de sécurité liées à la protection de sa personne ou de tiers, utiliser un nom qui ne lui appartient pas, ainsi qu'une qualité et une identité fictives, selon les modalités fixées par le Roi.	Un agent peut, pour des raisons de sécurité liées à la protection de sa personne ou de tiers, utiliser un **faux nom, une fausse qualité, une identité fictive ou une qualité fictive** ~~nom qui ne lui appartient pas, ainsi qu'une qualité et une identité fictives~~, selon les modalités fixées par le Roi.
La mesure visée à l'alinéa 1er ne peut pas être mise en œuvre de manière autonome pour la collecte de données.	La mesure visée à l'alinéa 1er ne peut pas être mise en œuvre de manière autonome pour la collecte de données.
Chaque utilisation active d'une identité fictive doit être temporaire et orientée vers l'objectif et est mentionnée dans une liste transmise mensuellement au Comité permanent R.	Chaque utilisation active d'une identité fictive doit être ~~**temporaire et**~~ orientée vers l'objectif et est mentionnée dans une liste transmise mensuellement au Comité permanent R.

Dans le cadre de la création et de l'utilisation d'un faux nom, d'une identité et d'une qualité fictives, les services de renseignement et de sécurité peuvent fabriquer, faire fabriquer et utiliser des faux documents.	Dans le cadre de la création et de l'utilisation d'un faux nom, **d'une fausse qualité,** d'une identité **ou** ~~et~~ d'une qualité fictives, les services de renseignement et de sécurité peuvent fabriquer, faire fabriquer et utiliser des faux documents.
Chaque création de documents officiels attestant d'une identité ou d'une qualité fictive est autorisée par le dirigeant du service et notifiée au Comité permanent R.	Chaque création de documents officiels attestant d'une identité ou d'une qualité fictive est autorisée par le dirigeant du service et notifiée au Comité permanent R.
Dans le cadre de l'exécution des mesures prévues au présent article, les services de renseignement et de sécurité peuvent requérir le concours des fonctionnaires et des agents des services publics.	Dans le cadre de l'exécution des mesures prévues au présent article, les services de renseignement et de sécurité peuvent requérir le concours des fonctionnaires et des agents des services publics.
	Sous-section 3.- La création et l'utilisation de personnes morales
Art. 13/3.	**Art. 13/3.**
§ 1er. Les services de renseignement et de sécurité 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.	§ 1er. Les services de renseignement et de sécurité 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.
§ 2. Les services de renseignement et de sécurité peuvent recourir à des personnes morales à l'appui de leurs missions.	§ 2. Les services de renseignement et de sécurité peuvent recourir à des personnes morales à l'appui de leurs missions.
Sans préjudice de l'alinéa 1er, les modalités du recours à une personne morale pour la collecte de données sont réglées à l'article 18/13.	Sans préjudice de l'alinéa 1er, les modalités du recours à une personne morale pour la collecte de données sont réglées à l'article 18/13.
§ 3. Dans le cadre de l'application des paragraphes 1er et 2, les services de renseignement et de sécurité peuvent fabriquer, faire fabriquer et utiliser des faux documents.	§ 3. Dans le cadre de l'application des paragraphes 1er et 2, les services de renseignement et de sécurité peuvent fabriquer, faire fabriquer et utiliser des faux documents.

§ 4. Chaque création d'une personne morale est autorisée par le dirigeant du service et notifiée au Comité permanent R.	§ 4. Chaque création d'une personne morale est autorisée par le dirigeant du service et notifiée au Comité permanent R.
Chaque recours à une personne morale hors le cas visé à l'article 18/13 est mentionné dans une liste transmise mensuellement au Comité permanent R.	Chaque recours à une personne morale hors le cas visé à l'article 18/13 est mentionné dans une liste transmise mensuellement au Comité permanent R.
§ 5. Dans le cadre de l'application du présent article, les services de renseignement et de sécurité peuvent requérir le concours des fonctionnaires et des agents des services publics.	§ 5. Dans le cadre de l'application du présent article, les services de renseignement et de sécurité peuvent requérir le concours des fonctionnaires et des agents des services publics.
	Sous-section 4.- Le concours de tiers
Art. 13/4.	**Art. 13/4.**
Les services de renseignement et de sécurité peuvent solliciter le concours de tiers.	Les services de renseignement et de sécurité peuvent solliciter le concours de tiers.
Les services veillent à la sécurité des données relatives aux tiers qui leur apportent ou leur ont apporté un concours.	Les services veillent à la sécurité des données relatives aux tiers qui leur apportent ou leur ont apporté un concours.
Les alinéas 2, 3 et 5 de l'article 13/1 sont applicables aux tiers qui ont fourni directement une aide ou une assistance nécessaire à l'exécution d'une méthode.	Les ~~alinéas 2, 3 et 5~~ **paragraphes 2 à 6 et 8 à 9** de l'article 13/1 **et le paragraphe 11 de l'article 13/1/1** sont applicables aux tiers qui ~~ont fourni~~ **fournissent** directement une aide ou une assistance nécessaire **pour l'application de la présente loi** ~~à l'exécution d'une méthode~~.
	L'aide et l'assistance apportées se font toujours sous le contrôle du service de renseignement et de sécurité concerné, qui garde la direction de l'opération.
Art. 16/3.	**Art. 16/3.**
§ 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de	§ 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs

leurs missions, décider de façon dûment motivée d'accéder aux données des passagers visées à l'article 27 de la loi du 25 décembre 2016 relative au traitement des données des passagers.	missions, décider de façon dûment motivée d'accéder aux données des passagers visées à l'article 27 de la loi du 25 décembre 2016 relative au traitement des données des passagers.
§ 2. La décision visée au § 1er est prise par le dirigeant du service et communiquée par écrit à l'Unité d'information des passagers visée au chapitre 7 de la loi précitée. La décision est notifiée au Comité permanent R avec la motivation de celle-ci.	§ 2. La décision visée au § 1er est prise par le dirigeant du service **ou son délégué** et communiquée par écrit à l'Unité d'information des passagers visée au chapitre 7 de la loi précitée. La décision est notifiée au Comité permanent R avec la motivation de celle-ci.
	En cas d'urgence, le dirigeant du service ou son délégué peut décider verbalement d'accéder à ces données. Cette décision verbale est confirmée par une décision écrite, le premier jour ouvrable qui suit la date de la décision, selon les modalités fixées à l'alinéa 1er.
Le Comite permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans les conditions qui ne respectent pas les conditions légales.	Le Comite permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans ~~les~~ **des** conditions qui ne respectent pas les ~~conditions~~ **dispositions** légales.
La décision peut porter sur un ensemble de données relatives à une enquête de renseignement spécifique. Dans ce cas, la liste des consultations des données des passagers est communiquée une fois par mois au Comité permanent R.	La décision peut porter sur un ensemble de données relatives à une enquête de renseignement spécifique. Dans ce cas, la liste des consultations des données des passagers est communiquée une fois par mois au Comité permanent R.
Art. 16/4.	**Art. 16/4.**
§ 1er. Selon les modalités déterminées par le Roi, après avis de l'autorité compétente de contrôle des traitements de données à caractère personnel, un accès direct est autorisé pour les services de renseignement et de sécurité aux informations et données à caractère personnel qui sont collectées au moyen de caméras dont l'utilisation par les services de police est autorisée conformément au chapitre IV, section 1re, et au chapitre IV/1, section 2, de la loi sur la fonction de police et qui sont notamment traitées dans les banques de données visées à l'article 44/2 de ladite loi.	§ 1er. Selon les modalités déterminées par le Roi, après avis de l'autorité compétente de contrôle des traitements de données à caractère personnel, un accès direct est autorisé pour les services de renseignement et de sécurité aux informations et données à caractère personnel qui sont collectées au moyen de caméras dont l'utilisation par les services de police est autorisée conformément au chapitre IV, section 1re, et au chapitre IV/1, section 2, de la loi sur la fonction de police et qui sont notamment traitées dans les banques de données visées à l'article 44/2 de ladite loi.

Par dérogation aux articles 25/5, § 2, et 46/2 de la loi sur la fonction de police, les services de police n'exercent pas de contrôle sur le visionnage en temps réel des images par les services de renseignement et de sécurité.	Par dérogation aux articles 25/5, § 2, et 46/2 de la loi sur la fonction de police, les services de police n'exercent pas de contrôle sur le visionnage en temps réel des images par les services de renseignement et de sécurité.
Après anonymisation, les informations et données à caractère personnel visées à l'alinéa 1er peuvent être utilisées à des fins didactiques et pédagogiques dans le cadre de la formation des membres des services de renseignement et de sécurité.	Après anonymisation, les informations et données à caractère personnel visées à l'alinéa 1er peuvent être utilisées à des fins didactiques et pédagogiques dans le cadre de la formation des membres des services de renseignement et de sécurité.
§ 2. Dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité peuvent accéder de manière ponctuelle et après leur enregistrement aux 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 loi sur la fonction de police, si cela est motivé sur le plan opérationnel, nécessaire pour l'exercice d'une mission précise et décidé par un officier de renseignement.	§ 2. Dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité peuvent accéder de manière ponctuelle et après leur enregistrement aux 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 loi sur la fonction de police, si cela est motivé sur le plan opérationnel, nécessaire pour l'exercice d'une mission précise et décidé par un officier **des méthodes** ~~de renseignement~~.
Après le premier mois de conservation, l'accès aux données visées au présent paragraphe est décidé par le dirigeant de service ou son délégué.	Après le premier mois de conservation, l'accès aux données visées au présent paragraphe est décidé par le dirigeant de service ou son délégué.
	En cas d'urgence, le dirigeant du service ou son délégué peut décider verbalement d'accéder à ces données. Cette décision verbale est confirmée par une décision écrite, le premier jour ouvrable qui suit la date de la décision, selon les modalités fixées à l'alinéa 4.
La décision du dirigeant de service ou de son délégué et sa motivation sont transmises au comité permanent R dans les meilleurs délais. La décision peut porter sur un ensemble de données relatives à une enquête de renseignement spécifique. Dans ce cas, une liste des accès ponctuels est communiquée une fois par mois au Comité permanent R. Le Comité permanent R interdit aux services de renseignement et de sécurité d'exploiter les	La décision du dirigeant de service ou de son délégué et sa motivation sont transmises au comité permanent R dans les meilleurs délais. La décision peut porter sur un ensemble de données relatives à une enquête de renseignement spécifique. Dans ce cas, une liste des accès ponctuels est communiquée une fois par mois au Comité permanent R. Le Comité permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans

données recueillies dans les conditions qui ne respectent pas les conditions légales.	~~les~~ **des** conditions qui ne respectent pas les ~~conditions~~ **dispositions** légales.
L'accès à ces informations et données à caractère personnel est protégé, tous les accès sont journalisés et les raisons concrètes des accès sont enregistrées.	L'accès à ces informations et données à caractère personnel est protégé, tous les accès sont journalisés et les raisons concrètes des accès sont enregistrées.
§ 3. Dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité peuvent mettre les informations et données à caractère personnel des banques de données visées à l'article 44/2, § 3, alinéa 2, 1° et 2°, de la loi sur la fonction de police en corrélation avec :	§ 3. Dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité peuvent mettre les informations et données à caractère personnel des banques de données visées à l'article 44/2, § 3, alinéa 2, 1° et 2°, de la loi sur la fonction de police en corrélation avec :
1° les banques de données gérées par les services de renseignement et de sécurité ou qui leur sont directement disponibles ou accessibles dans le cadre de leurs missions, ou des listes de personnes élaborées par les services de renseignement et de sécurité dans le cadre de leurs missions ;	1° les banques de données gérées par les services de renseignement et de sécurité ou qui leur sont directement disponibles ou accessibles dans le cadre de leurs missions, ou des listes de personnes élaborées par les services de renseignement et de sécurité dans le cadre de leurs missions ;
2° des critères d'évaluation préétablis. Les banques de données ou les listes, ou les critères d'évaluation préétablis visés au présent paragraphe sont préparés dans le but de réaliser cette corrélation après enregistrement des données.	2° des critères d'évaluation préétablis. Les banques de données ou les listes, ou les critères d'évaluation préétablis visés au présent paragraphe sont préparés dans le but de réaliser cette corrélation après enregistrement des données.
Le contenu des banques de données ou des listes visées à l'alinéa 1er, 1°, utilisées en vue d'une corrélation, est soumis à l'autorisation d'un officier de renseignement. La décision de mettre les banques de données ou les listes en corrélation peut porter sur un ensemble de données relatives à une ou plusieurs enquêtes de renseignement spécifiques.	Le contenu des banques de données ou des listes visées à l'alinéa 1er, 1°, utilisées en vue d'une corrélation, est soumis à l'autorisation d'un officier **des méthodes** ~~de renseignement~~. La décision de mettre les banques de données ou les listes en corrélation peut porter sur un ensemble de données relatives à une ou plusieurs enquêtes de renseignement spécifiques.
Chaque liste avec laquelle la corrélation visée à l'alinéa 1er, 1°, est réalisée, est communiquée dans les meilleurs délais au Comité permanent	Chaque liste avec laquelle la corrélation visée à l'alinéa 1er, 1°, est réalisée, est communiquée dans les meilleurs délais au Comité permanent R.

R. Le Comité permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans les circonstances qui ne respectent pas les conditions légales.	Le Comité permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans ~~les~~ **des conditions** ~~circonstances~~ qui ne respectent pas les **dispositions** ~~conditions~~ légales.
Les critères d'évaluation visés à l'alinéa 1er, 2°, sont préalablement présentés au Comité permanent R. Des corrélations qui affinent ces critères d'évaluations ne doivent plus être présentées. Ces critères d'évaluation ne peuvent viser l'identification d'un individu et doivent être ciblés, proportionnés et spécifiques.	Les critères d'évaluation visés à l'alinéa 1er, 2°, sont préalablement présentés au Comité permanent R. Des corrélations qui affinent ces critères d'évaluations ne doivent plus être présentées. Ces critères d'évaluation ne peuvent viser l'identification d'un individu et doivent être ciblés, proportionnés et spécifiques.
§ 4. Dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité peuvent accéder au registre mentionné à l'article 25/8, alinéa 2, de la loi sur la fonction de police.	§ 4. Dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité peuvent accéder au registre mentionné à l'article 25/8, alinéa 2, de la loi sur la fonction de police.
§ 5. Dans le cas où l'accès direct visé au présent article est possible, un service de renseignement et de sécurité ne peut pas solliciter le même accès direct sur la base de l'article 14, alinéa 2.	§ 5. Dans le cas où l'accès direct visé au présent article est possible, un service de renseignement et de sécurité ne peut pas solliciter le même accès direct sur la base de l'article 14, alinéa 2.
Le magistrat compétent qui estime qu'un accès direct aux informations et aux données à caractère personnel entrave la bonne exécution d'une enquête ou d'une instruction judiciaire, peut décider de suspendre temporairement l'accès. Si un service de renseignement ou de sécurité utilise un accès direct concernant ces informations et données à caractère personnel, il sera informé que ces dernières sont incomplètes.	Le magistrat compétent qui estime qu'un accès direct aux informations et aux données à caractère personnel entrave la bonne exécution d'une **information** ~~enquête~~ ou d'une instruction judiciaire, peut décider de suspendre temporairement l'accès. Si un service de renseignement ou de sécurité utilise un accès direct concernant ces informations et données à caractère personnel, il sera informé que ces dernières sont incomplètes.
§ 6. L'officier de renseignement qui prend les décisions prévues par cet article, ne peut pas être en même temps le gestionnaire du dossier auquel la décision se rapporte.	§ 6. L'officier **des méthodes** ~~de renseignement~~ qui prend les décisions prévues par cet article, ne peut pas être en même temps le gestionnaire du dossier auquel la décision se rapporte.

Art. 16/5.	**Art. 16/5.**
	Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, s'infiltrer dans le monde virtuel, sous couvert ou non d'un faux nom ou d'une fausse qualité.
Art. 16/6.	**Art. 16/6.**
	§ 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours :
	1° des personnes et institutions visées à l'article 5, paragraphe 1er, 3° à 22°, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces ;
	2° des personnes et institutions qui, sur le territoire belge, mettent à disposition ou proposent des services en lien avec des valeurs virtuelles permettant d'échanger des moyens de paiement réglementés en valeurs virtuelles ;
	3° du Point de Contact Central tenu par la Banque nationale de Belgique conformément à la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt ;
	afin de procéder à :
	a) l'identification des produits et services dont la personne visée est le titulaire, le mandataire ou le bénéficiaire effectif;

	b) l'identification des titulaires, des mandataires ou des bénéficiaires effectifs des produits et services.
	Le dirigeant du service ou son délégué effectue la réquisition, visée au premier alinéa, 1° et 2°, par écrit. En cas d'extrême urgence, le dirigeant du service ou son délégué peut requérir ces données verbalement. Cette réquisition verbale doit être confirmée par écrit dans un délai de vingt-quatre heures.
	La coopération requise visée à l'alinéa 1er, 3 ° a lieu après une décision écrite du dirigeant du service ou de son délégué, et conformément à la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt. En cas d'extrême urgence, le dirigeant du service ou son délégué peut autoriser verbalement la méthode. Cette décision verbale est confirmée par une décision écrite dans un délai de vingt-quatre heures.
	§ 2. La personne ou l'institution requise est tenue de remettre sans délai les informations demandées après réception de la réquisition écrite du dirigeant du service ou de son délégué.
	La personne ou l'institution requise qui refuse de prêter le concours visé au présent article est punie d'une amende de vingt-six euros à vingt mille euros.
	§ 3. Les deux services de renseignement et de sécurité tiennent un registre de toutes les identifications requises. Le service de renseignement et de sécurité concerné transmet chaque mois au Comité permanent R une liste des identifications requises.

	Le Comité permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans des conditions qui ne respectent pas les dispositions légales.
Art. 18.	**Art. 18.**
Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, avoir recours à des sources humaines pour la collecte de données en rapport avec des événements, des objets, des groupements et des personnes physiques ou morales présentant un intérêt pour l'exercice de leurs missions, conformément aux directives du Conseil national de sécurité.	**§1.** Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, avoir recours **à des personnes dont** des sources humaines pour la collecte de données en rapport avec des événements, des objets, des groupements et des personnes physiques ou morales présentant un intérêt pour l'exercice de leurs missions, conformément aux directives du Conseil national de sécurité.
	§2. Dans l'intérêt de l'exercice de leurs missions visées aux articles 7, 1° et 3°/1 et 11, §1er, 1° à 3° et 5°, les services de renseignement et de sécurité peuvent mettre en œuvre des méthodes de recueil de données à l'égard d'une source humaine.
	1° lorsqu'il y a un doute quant à sa fiabilité, sa discrétion ou sa loyauté vis-à-vis du service de renseignement et de sécurité concerné susceptible de causer un préjudice pour l'exercice des missions dudit service, ou
	2° pour assurer sa protection.
Art. 18/1	**Art. 18/1**
La présente sous-section s'applique :	La présente sous-section s'applique :
1° à la Sûreté de l'Etat pour l'exercice, sur ou à partir du territoire du Royaume, des missions visées aux articles 7, 1° et 3° /1, […], sans préjudice de l'article 18/9, § 1er, 1°;	1° à la Sûreté de l'Etat pour l'exercice, sur ou à partir du territoire du Royaume, des missions visées aux articles 7, 1° et 3° /1, […], sans préjudice de l'article 18/9, § 1er, 1°;
2° au Service Général du Renseignement et de la Sécurité, sans préjudice de l'article 18/9, § 1er, 2°, pour l'exercice des missions visées aux articles 11, § 1er, 1° à 3° et 5°, et § 2, à	2° au Service Général du Renseignement et de la Sécurité, sans préjudice de l'article 18/9, § 1er, 2°, pour l'exercice des missions visées aux articles 11, § 1er, 1° à 3° et 5°, et § 2, à l'exception de

l'exception de l'interception de communications émises ou reçues à l'étranger et de l'intrusion dans un système informatique situé à l'étranger et de la prise d'images fixes ou animées effectuée à l'étranger, visées aux articles 44 à 44/5.	l'interception de communications émises ou reçues à l'étranger et de l'intrusion dans un système informatique situé à l'étranger et de la prise d'images fixes ou animées effectuée à l'étranger, visées aux articles 44 à 44/5~~.~~**;**
	3° sans préjudice des 1° et 2°, aux services de renseignement et de sécurité, dans le cadre de l'article 18, §2.
Art. 18/2	**Art. 18/2**
§ 1er. Les méthodes spécifiques de recueil de données sont énumérées aux articles 18/4 à 18/8.	§ 1er. Les méthodes spécifiques de recueil de données sont énumérées aux articles 18/4 à 18/8.
§ 2. Les méthodes exceptionnelles de recueil de données sont énumérées aux articles 18/11 à 18/17.	§ 2. Les méthodes exceptionnelles de recueil de données sont énumérées aux articles 18/11 à 18/17.
§ 3. Si une méthode visée aux § § 1er et 2 est mise en œuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de leurs locaux ou de moyens de communication qu'ils utilisent à des fins professionnelles, ou de leur résidence, ou de leur domicile, cette méthode ne peut être exécutée sans que, suivant le cas, le président de l'Ordre des barreaux francophones et germanophone ou le président de l'Orde van Vlaamse balies, le président du Conseil national de l'Ordre des médecins ou le président de l'Association des journalistes professionnels, ou leur suppléant en cas de maladie ou d'empêchement du président en soit averti au préalable par le président de la commission visée à l'article 3, 6° ou, en cas d'empêchement, par un autre membre de la Commission. Le président de la commission ou le membre de la Commission qui remplace le président est tenu de fournir les informations nécessaires au président de l'Ordre ou de l'association des journalistes professionnels dont fait partie l'avocat, le médecin ou le journaliste ou à son suppléant. Le président concerné et son suppléant sont tenus au secret. Les peines prévues à l'article	§ 3. Si une méthode visée aux ~~§ §~~paragraphes 1er et 2 est mise en œuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de leurs locaux ou de moyens de communication qu'ils utilisent à des fins professionnelles, ou de leur résidence, ou de leur domicile, cette méthode ne peut être exécutée sans que, suivant le cas, le président de l'Ordre des barreaux francophones et germanophone ou le président de l'Orde van Vlaamse balies, le président du Conseil national de l'Ordre des médecins ou le président de l'Association des journalistes professionnels, ou leur suppléant en cas de maladie ou d'empêchement du président en soit averti au préalable par le président de la commission visée à l'article 3, 6° ou, en cas d'empêchement, par un autre membre de la Commission. Le président de la commission ou le membre de la Commission qui remplace le président est tenu de fournir les informations nécessaires au président de l'Ordre ou de l'association des journalistes professionnels dont fait partie l'avocat, le médecin ou le journaliste ou à son suppléant. Le président concerné et son suppléant sont tenus au secret. Les peines prévues à l'article 458 du Code pénal

458 du Code pénal s'appliquent aux infractions à cette obligation de garder le secret.	s'appliquent aux infractions à cette obligation de garder le secret.
Si une méthode visée aux §§ 1er et 2 est mise en œuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de leurs locaux ou de moyens de communication qu'ils utilisent à des fins professionnelles, ou de leur résidence ou de leur domicile, le président de la commission vérifie si les données obtenues grâce à cette méthode, lorsqu'elles sont protégées par le secret professionnel de l'avocat ou du médecin ou par le secret des sources du journaliste, sont directement liées à la menace potentielle. Si aucun lien direct n'est démontré, la Commission interdit aux services de renseignement et de sécurité d'exploiter ces données.	Si une méthode visée aux ~~§§~~**paragraphes** 1er et 2 est mise en œuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de leurs locaux ou de moyens de communication qu'ils utilisent à des fins professionnelles, ou de leur résidence ou de leur domicile, le président de la commission **ou, en cas d'empêchement, un autre membre de la Commission** vérifie si les données obtenues grâce à cette méthode, lorsqu'elles sont protégées par le secret professionnel de l'avocat ou du médecin ou par le secret des sources du journaliste, sont directement liées à la menace potentielle. Si aucun lien direct n'est démontré, la Commission interdit aux services de renseignement et de sécurité d'exploiter ces données.
Si une méthode exceptionnelle visée au § 2 est mise en œuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, le président de la commission ou le membre de la commission délégué par lui peut être présent lors de la mise en œuvre de la méthode. Le président tient compte du risque que sa présence peut occasionner pour l'exécution de la mission, sa propre sécurité et celle des agents et des tiers.	Si une méthode exceptionnelle visée au ~~§~~ **paragraphe** 2 est mise en œuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, le président de la commission ou le membre de la commission délégué par lui peut être présent lors de la mise en œuvre de la méthode. Le président tient compte du risque que sa présence peut occasionner pour l'exécution de la mission, sa propre sécurité et celle des agents et des tiers.
	§4. Lorsqu'une méthode visée aux paragraphes 1er et 2 est mise en œuvre à l'égard d'une source humaine en application de l'article 18, § 2, il est dérogé aux mentions prescrites sous peine de nullité prévues aux articles 18/3, §2, 2° et 3° et 18/10, §2, 2° et 3°.
Art. 18/3	**Art. 18/3**
§ 1er. Les méthodes spécifiques de recueil de données visées à l'article 18/2, § 1er, peuvent être mises en œuvre compte tenu de la menace potentielle visée à l'article 18/1 si les méthodes ordinaires de recueil de données sont jugées insuffisantes pour permettre de	§ 1er. Les méthodes spécifiques de recueil de données visées à l'article 18/2, § 1er, peuvent être mises en œuvre compte tenu de la menace potentielle visée à l'article 18/1 **ou dans le cadre de l'article 18, § 2,** si les méthodes ordinaires de recueil de données sont jugées insuffisantes pour

récolter les informations nécessaires à l'aboutissement d'une mission de renseignement. La méthode spécifique doit être choisie en fonction du degré de gravité de la menace potentielle pour laquelle elle est mise en œuvre.	permettre de récolter les informations nécessaires à l'aboutissement d'une mission de renseignement. La méthode spécifique doit être choisie en fonction du degré de gravité de la menace potentielle pour laquelle elle est mise en œuvre **ou en fonction du degré de gravité du préjudice potentiel pour l'exercice des missions des services ou du danger potentiel pour la sécurité de la source humaine dans le cadre de l'article 18, §2**.
La méthode spécifique ne peut être mise en œuvre qu'après décision écrite et motivée du dirigeant du service et après notification de cette décision à la commission.	La méthode spécifique ne peut être mise en œuvre qu'après décision écrite et motivée du dirigeant du service et après notification de cette décision à la commission.
§ 2. La décision du dirigeant du service mentionne :	§ 2. La décision du dirigeant du service mentionne :
1° la nature de la méthode spécifique ;	1° la nature de la méthode spécifique ;
2° selon le cas, les personnes physiques ou morales, les associations de fait ou les groupements, les objets, les lieux, les événements ou les informations**,** soumis à la méthode spécifique ;	2° selon le cas, les personnes physiques ou morales, les associations de fait ou les groupements, les objets, les lieux, les événements ou les informations**,** soumis à la méthode spécifique ;
3° la menace potentielle qui justifie la méthode spécifique;	3° la menace potentielle qui justifie la méthode spécifique;
4° les circonstances de fait qui justifient la méthode spécifique, la motivation en matière de subsidiarité et de proportionnalité, en ce compris le lien entre le 2° et le 3° ;	4° les circonstances de fait qui justifient la méthode spécifique, la motivation en matière de subsidiarité et de proportionnalité, en ce compris le lien entre le 2° et le 3° ;
5° la période pendant laquelle la méthode spécifique peut être appliquée, à compter de la notification de la décision à la Commission ;	5° la période pendant laquelle la méthode spécifique peut être appliquée, à compter de la notification de la décision à la Commission ;

6° le nom du (ou des) officier(s) des méthodes renseignement responsable(s) pour le suivi de la mise en œuvre de la méthode spécifique ;	6° le nom du (ou des) officier(s) des méthodes renseignement responsable(s) pour le suivi de la mise en œuvre de la méthode spécifique ;
7° le cas échéant, le moyen technique employé pour mettre en œuvre la méthode spécifique en application des articles 18/4 ou 18/5 ;	7° le cas échéant, le moyen technique employé pour mettre en œuvre la méthode spécifique en application des articles 18/4 ou 18/5 ;
8° le cas échéant, le concours avec une information ou une instruction judiciaire ;	8° le cas échéant, le concours avec une information ou une instruction judiciaire ;
9° le cas échéant, les infractions absolument nécessaires afin d'assurer l'exécution optimale de la méthode ou de garantir la sécurité des agents ou de tiers ;	9° le cas échéant, ~~les infractions~~ **les faits susceptibles d'être qualifiés infraction(s)** absolument nécessaires afin d'assurer l'exécution optimale de la méthode ou de garantir la sécurité des agents ou de tiers ;
10° le cas échéant, les indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle ;	10° le cas échéant, les indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle ;
11° le cas échéant, les motifs qui justifient l'extrême urgence ;	11° le cas échéant, les motifs qui justifient l'extrême urgence ;
12° dans le cas où il est fait application de l'article 18/8, la motivation de la durée de la période à laquelle a trait la collecte de données ;	12° dans le cas où il est fait application de l'article 18/8, la motivation de la durée de la période à laquelle a trait la collecte de données ;
13° la date de la décision ;	13° la date de la décision ;
14° la signature du dirigeant du service.	14° la signature du dirigeant du service.
Les mentions visées aux 1° à 4°, 7°, 9°, 10°, 11° et 14° sont prescrites sous peine d'illégalité.	Les mentions visées aux 1° à 4°, 7°, 9°, 10°, 11° et 14° sont prescrites sous peine d'illégalité.
	Dans le cadre de l'article 18 §2 et par dérogation au paragraphe 2, 2° et 3°, la décision du dirigeant du service mentionne respectivement le code d'identification de la source humaine et le préjudice potentiel pour l'exercice des missions

	des services ou le danger potentiel pour la sécurité de la source humaine.
§ 3. En cas d'extrême urgence, le dirigeant du service peut autoriser verbalement la méthode spécifique. Cette décision verbale est confirmée par une décision écrite motivée comprenant les mentions prévues au paragraphe 2 et qui doit parvenir au siège de la Commission au plus tard le premier jour ouvrable qui suit la date de la décision.	§ 3. En cas d'extrême urgence, le dirigeant du service peut autoriser verbalement la méthode spécifique. Cette décision verbale est confirmée par une décision écrite motivée comprenant les mentions prévues au paragraphe 2 et qui doit parvenir au siège de la Commission au plus tard le premier jour ouvrable qui suit la date de la décision.
L'officier de renseignement peut requérir verbalement ou par écrit le concours des personnes visées aux articles 18/6, 18/7 et 18/8. La nature de la méthode leur est communiquée. En cas de réquisition verbale, celle- ci est confirmée par écrit dans les plus brefs délais par l'officier de renseignement.	L'officier **des méthodes** ~~de renseignement~~ peut requérir verbalement ou par écrit le concours des personnes visées aux articles 18/6, **18/6/1,** 18/7 et 18/8. La nature de la méthode leur est communiquée. En cas de réquisition verbale, celle-ci est confirmée par écrit dans les plus brefs délais par l'officier **des méthodes** ~~de renseignement~~.
§ 4. L'utilisation de la méthode spécifique ne peut être prolongée ou renouvelée que moyennant une nouvelle décision du dirigeant du service qui répond aux conditions prévues au § 1er.	§ 4. L'utilisation de la méthode spécifique ne peut être prolongée ou renouvelée que moyennant une nouvelle décision du dirigeant du service qui répond aux conditions prévues au § 1er.
§ 5. Les méthodes spécifiques ne peuvent être mise en œuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de moyens de communication que ceux-ci utilisent à des fins professionnelles qu'à la condition que le service de renseignement et de sécurité dispose au préalable d'indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle et après que la commission a rendu, conformément à l'article 18/10, un avis conforme sur le projet de décision du dirigeant du service.	§ 5. Les méthodes spécifiques ne peuvent être mise en œuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de moyens de communication que ceux-ci utilisent à des fins professionnelles qu'à la condition que le service de renseignement et de sécurité dispose au préalable d'indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle et après que la commission a rendu, conformément à l'article 18/10, un avis conforme sur le projet de décision du dirigeant du service.
§ 6. Les membres de la commission peuvent contrôler à tout moment la légalité des mesures, y compris le respect des principes de subsidiarité et de proportionnalité.	§ 6. Les membres de la commission peuvent contrôler à tout moment la légalité des ~~mesures, y compris le respect des principes de subsidiarité et de proportionnalité~~ **méthodes spécifiques de recueil de données, y compris le respect des**

	principes de subsidiarité et de proportionnalité prévu à l'article 18/3, §1er.
Ils peuvent, à cet effet, pénétrer dans les lieux où sont réceptionnées ou conservées les données relatives aux méthodes spécifiques, se saisir de toutes les pièces utiles et entendre les membres du service.	Ils peuvent, à cet effet, pénétrer dans les lieux où sont réceptionnées ou conservées les données relatives aux méthodes spécifiques, se saisir de toutes les pièces utiles et entendre les membres du service.
Les données recueillies dans des conditions qui ne respectent pas les dispositions légales en vigueur sont conservées sous le contrôle de la commission, selon les modalités et les délais fixés par le Roi, après avis de la commission de la protection de la vie privée. La commission interdit aux services de renseignement et de sécurité d'exploiter ces données et suspend la méthode mise en œuvre si celle-ci est toujours en cours.	Les données recueillies dans des conditions qui ne respectent pas les dispositions légales en vigueur sont conservées sous le contrôle de la commission, selon les modalités et les délais fixés par le Roi, après avis ~~de la commission de la protection de la vie privée~~ **du Comité permanent R**. La commission interdit aux services de renseignement et de sécurité d'exploiter ces données et suspend la méthode mise en œuvre si celle-ci est toujours en cours.
La commission notifie de sa propre initiative et sans délai sa décision au Comité permanent R.	La commission notifie de sa propre initiative et sans délai sa décision au Comité permanent R.
§ 7. L'officier de renseignement désigné pour le suivi de la mise en œuvre la méthode spécifique de recueil de données informe régulièrement le dirigeant du service de l'exécution de cette méthode.	§ 7. L'officier **des méthodes** ~~de renseignement~~ désigné pour le suivi de la mise en œuvre la méthode spécifique de recueil de données informe régulièrement le dirigeant du service de l'exécution de cette méthode.
§ 8. Le dirigeant du service met fin à la méthode spécifique lorsque la menace potentielle qui la justifie a disparu, lorsque la méthode n'est plus utile pour la finalité pour laquelle elle avait été mise en œuvre, ou quand il a constaté une illégalité. Il informe dans les plus brefs délais la Commission de sa décision.	§ 8. Le dirigeant du service met fin à la méthode spécifique lorsque la menace potentielle qui la justifie a disparu, lorsque la méthode n'est plus utile pour la finalité pour laquelle elle avait été mise en œuvre, ou quand il a constaté une illégalité. Il informe dans les plus brefs délais la Commission de sa décision.
Art. 18/5/1	**Art. 18/5/1**
	Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, s'infiltrer dans le monde virtuel sous couvert d'une identifié fictive ou d'une qualité fictive.

Art. 18/9	**Art. 18/9**
§ 1er. Les méthodes exceptionnelles de recueil des données visées à l'article 18/2, § 2, peuvent être mises en œuvre :	§ 1er. Les méthodes exceptionnelles de recueil des données visées à l'article 18/2, § 2, peuvent être mises en œuvre :
1° par la Sûreté de l'Etat, lorsqu'il existe une menace potentielle grave contre un intérêt fondamental de l'Etat visé à l'article 8, 2° à 4°, et lorsque cette menace potentielle est liée à une activité visée à l'article 8, 1° ou est liée à une activité d'un service de renseignement étranger ;	1° par la Sûreté de l'Etat, lorsqu'il existe une menace potentielle grave contre un intérêt fondamental de l'Etat visé à l'article 8, 2° à 4°, et lorsque cette menace potentielle est liée à une activité visée à l'article 8, 1° ou est liée à une activité d'un service de renseignement étranger **ou dans le cadre de l'article 18, § 2 lorsqu'il existe un préjudice potentiel grave pour l'exercice des missions des services ou un danger potentiel grave pour la sécurité de la source humaine**;
2° par le Service Général du Renseignement et de la Sécurité lorsqu'il existe une menace potentielle grave contre un intérêt fondamental visé à l'article 11, § 1er, 1° à 3° et 5°, à l'exception de tout autre intérêt fondamental du pays défini par le Roi visé à l'article 11, § 1er, 1°, f).	2° par le Service Général du Renseignement et de la Sécurité lorsqu'il existe une menace potentielle grave contre un intérêt fondamental visé à l'article 11, § 1er, 1° à 3° et 5°, à l'exception de tout autre intérêt fondamental du pays défini par le Roi visé à l'article 11, § 1er, 1°, f) **ou dans le cadre de l'article 18, § 2 lorsqu'il existe un préjudice potentiel grave pour l'exercice des missions des services ou un danger potentiel grave pour la sécurité de la source humaine.**
§ 2. A titre exceptionnel et compte tenu d'une menace potentielle visée au paragraphe 1er, les méthodes exceptionnelles de recueil de données visées à l'article 18/2, § 2, ne peuvent être mises en œuvre que si les méthodes ordinaires et spécifiques de recueil de données sont jugées insuffisantes pour permettre de recueillir les informations nécessaires à l'aboutissement d'une mission de renseignement.	§ 2. A titre exceptionnel et compte tenu d'une menace**, d'un préjudice ou d'un danger potentiel visé** ~~potentielle visée~~ au paragraphe 1er, les méthodes exceptionnelles de recueil de données visées à l'article 18/2, § 2, ne peuvent être mises en œuvre que si les méthodes ordinaires et spécifiques de recueil de données sont jugées insuffisantes pour permettre de recueillir les informations nécessaires à l'aboutissement d'une mission de renseignement.
Le dirigeant du service ne peut autoriser la mise en œuvre d'une méthode exceptionnelle qu'après avis conforme de la commission.	Le dirigeant du service ne peut autoriser la mise en œuvre d'une méthode exceptionnelle qu'après avis conforme de la commission.

§ 3. La méthode exceptionnelle doit être choisie en fonction du degré de gravité que représente la menace potentielle.	§ 3. La méthode exceptionnelle doit être choisie en fonction du degré de gravité que représente la menace potentielle **ou en fonction du degré de gravité du préjudice potentiel pour l'exercice des missions des services ou du danger potentiel pour la sécurité de la source humaine dans le cadre de l'article 18 §2.**
§ 4. Les méthodes exceptionnelles ne peuvent être mises en œuvre à l'égard d'un avocat, d'un médecin, d'un journaliste, ou des locaux ou moyens de communications qu'ils utilisent à des fins professionnelles, ou de leur résidence, ou de leur domicile qu'à la condition que le service de renseignement et de sécurité dispose préalablement d'indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement d'une menace potentielle grave visée au paragraphe 1er.	§ 4. Les méthodes exceptionnelles ne peuvent être mises en œuvre à l'égard d'un avocat, d'un médecin, d'un journaliste, ou des locaux ou moyens de communications qu'ils utilisent à des fins professionnelles, ou de leur résidence, ou de leur domicile qu'à la condition que le service de renseignement et de sécurité dispose préalablement d'indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement d'une menace potentielle grave visée au paragraphe 1er.
Art. 18/10	**Art. 18/10**
§ 1er. Le dirigeant du service soumet son projet d'autorisation à l'avis conforme de la commission, qui vérifie si les dispositions légales relatives à l'utilisation de la méthode exceptionnelle pour le recueil de données, ainsi que les principes de subsidiarité et de proportionnalité prévus à l'article 18/9 § § 2 et 3, sont respectés et qui contrôle les mentions prescrites par le § 2.	§ 1er. Le dirigeant du service soumet son projet d'autorisation à l'avis conforme de la commission, qui vérifie si les dispositions légales relatives à l'utilisation de la méthode exceptionnelle pour le recueil de données, ainsi que les principes de subsidiarité et de proportionnalité prévus à l'article 18/9 § § 2 et 3, sont respectés et qui contrôle les mentions prescrites par le § 2.
Sauf disposition légale contraire, la période durant laquelle la méthode exceptionnelle de recueil de données peut être appliquée ne peut excéder deux mois, à compter de l'autorisation, sans préjudice de la possibilité de prolongation prévue au § 5.	Sauf disposition légale contraire, la période durant laquelle la méthode exceptionnelle de recueil de données peut être appliquée ne peut excéder deux mois, à compter de l'autorisation, sans préjudice de la possibilité de prolongation prévue au § 5.
L'officier de renseignement désigné pour le suivi de la mise en œuvre de la méthode exceptionnelle de recueil de données informe régulièrement le dirigeant du service, qui, à son tour, informe la commission de l'exécution de	L'officier **des méthodes** ~~de renseignement~~ désigné pour le suivi de la mise en œuvre de la méthode exceptionnelle de recueil de données informe régulièrement le dirigeant du service, qui, à son tour, informe la commission de l'exécution de

cette méthode, selon les modalités et délais déterminés par le Roi.	cette méthode, selon les modalités et délais déterminés par le Roi.
Le dirigeant du service met fin à la méthode exceptionnelle lorsque la menace potentielle grave qui la justifie a disparu, lorsque la méthode n'est plus utile pour la finalité pour laquelle elle avait été mise en œuvre, ou quand il a constaté une illégalité. Il informe dès que possible la Commission de sa décision.	Le dirigeant du service met fin à la méthode exceptionnelle lorsque la menace potentielle grave qui la justifie a disparu, lorsque la méthode n'est plus utile pour la finalité pour laquelle elle avait été mise en œuvre, ou quand il a constaté une illégalité. Il informe dès que possible la Commission de sa décision.
§ 2. Le projet d'autorisation du dirigeant du service mentionne:	§ 2. Le projet d'autorisation du dirigeant du service mentionne:
1° la nature de la méthode exceptionnelle;	1° la nature de la méthode exceptionnelle;
2° selon le cas, la ou les personnes physiques ou morales, les associations de fait ou les groupements, les objets, les lieux, les événements ou les informations faisant l'objet de la méthode exceptionnelle de recueil de données ;	2° selon le cas, la ou les personnes physiques ou morales, les associations de fait ou les groupements, les objets, les lieux, les événements ou les informations faisant l'objet de la méthode exceptionnelle de recueil de données ;
3° la menace potentielle grave qui justifie la méthode exceptionnelle de recueil de données;	3° la menace potentielle grave qui justifie la méthode exceptionnelle de recueil de données;
4° les circonstances de fait qui justifient la méthode exceptionnelle, la motivation en matière de subsidiarité et de proportionnalité, en ce compris le lien entre le 2° et le 3° ;	4° les circonstances de fait qui justifient la méthode exceptionnelle, la motivation en matière de subsidiarité et de proportionnalité, en ce compris le lien entre le 2° et le 3° ;
5° la période pendant laquelle la méthode exceptionnelle de recueil de données peut être mise en œuvre à compter de l'autorisation du dirigeant du service;	5° la période pendant laquelle la méthode exceptionnelle de recueil de données peut être mise en œuvre à compter de l'autorisation du dirigeant du service;
6° le nom du ou des officier(s) de renseignement désigné(s) pour le suivi de la mise en œuvre de la méthode exceptionnelle;	6° le nom du ou des officier(s) **des méthodes** ~~de renseignement~~ désigné(s) pour le suivi de la mise en œuvre de la méthode exceptionnelle;

7° le cas échéant, le moyen technique employé pour mettre en œuvre la méthode exceptionnelle en application des articles 18/11 ou 18/12;	7° le cas échéant, le moyen technique employé pour mettre en œuvre la méthode exceptionnelle en application des articles 18/11 ou 18/12;
8° le cas échéant, le concours d'une information ou d'une instruction judiciaire;	8° le cas échéant, le concours d'une information ou d'une instruction judiciaire;
9° le cas échéant, les infractions absolument nécessaires afin d'assurer l'exécution optimale de la méthode ou de garantir la sécurité des agents ou de tiers;	9° le cas échéant, ~~les infractions~~ **les faits susceptibles d'être qualifiés infraction(s)** absolument nécessaires afin d'assurer l'exécution optimale de la méthode ou de garantir la sécurité des agents ou de tiers;
10° le cas échéant, les indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle;	10° le cas échéant, les indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle;
11° le cas échéant, les motifs qui justifient l'extrême urgence;	11° le cas échéant, les motifs qui justifient l'extrême urgence;
12° la date de l'autorisation;	12° la date de l'autorisation;
13° la signature du dirigeant du service.	13° la signature du dirigeant du service.
Les mentions visées à l'alinéa 1er sont prescrites sous peine d'illégalité.	Les mentions visées à l'alinéa 1er sont prescrites sous peine d'illégalité.
	Dans le cadre de l'article 18 §2 et par dérogation au paragraphe 2, 2° et 3°, la décision du dirigeant du service mentionne respectivement le code d'identification de la source humaine et le préjudice potentiel grave pour l'exercice des missions des services ou le danger potentiel grave pour la sécurité de la source humaine.

§ 3. La commission donne son avis conforme dans les quatre jours de la réception du projet d'autorisation.	§ 3. La commission donne son avis conforme dans les quatre jours de la réception du projet d'autorisation.
Si la commission rend un avis négatif, la méthode exceptionnelle de recueil de données ne peut pas être mise en œuvre par le service concerné.	Si la commission rend un avis négatif, la méthode exceptionnelle de recueil de données ne peut pas être mise en œuvre par le service concerné.
Si la commission ne rend pas d'avis dans le délai de quatre jours ou informe le service concerné qu'elle est dans l'impossibilité de délibérer dans ce délai conformément à l'article 43, paragraphe 1er, alinéa 7, le service concerné peut saisir le ministre compétent, qui autorisera ou n'autorisera pas la mise en œuvre dans les plus brefs délais de la méthode envisagée. Le ministre communique sa décision aux présidents de la commission et du Comité permanent R.	Si la commission ne rend pas d'avis dans le délai de quatre jours ou informe le service concerné qu'elle est dans l'impossibilité de délibérer dans ce délai conformément à l'article 43, paragraphe 1er, alinéa 7, le service concerné peut saisir le ministre compétent, qui autorisera ou n'autorisera pas la mise en œuvre dans les plus brefs délais de la méthode envisagée. Le ministre communique sa décision aux présidents de la commission et du Comité permanent R.
Le dirigeant du service informe le ministre du suivi de la méthode exceptionnelle ainsi autorisée en lui faisant, selon une périodicité fixée par le ministre dans son autorisation, un rapport circonstancié sur le déroulement de la méthode.	Le dirigeant du service informe le ministre du suivi de la méthode exceptionnelle ainsi autorisée en lui faisant, selon une périodicité fixée par le ministre dans son autorisation, un rapport circonstancié sur le déroulement de la méthode.
Le ministre concerné met fin à la méthode exceptionnelle qu'il a autorisée lorsque la menace potentielle qui la justifie a disparu ou si la méthode en question ne s'avère plus utile à la finalité pour laquelle elle a été décidée. Il suspend la méthode lorsqu'il constate une illégalité. Dans ce cas, le ministre concerné porte sans délai à la connaissance de la commission, du dirigeant du service et du Comité permanent R sa décision motivée de mettre fin à la méthode exceptionnelle ou de la suspendre, selon le cas.	Le ministre concerné met fin à la méthode exceptionnelle qu'il a autorisée lorsque la menace potentielle qui la justifie a disparu ou si la méthode en question ne s'avère plus utile à la finalité pour laquelle elle a été décidée. Il suspend la méthode lorsqu'il constate une illégalité. Dans ce cas, le ministre concerné porte sans délai à la connaissance de la commission, du dirigeant du service et du Comité permanent R sa décision motivée de mettre fin à la méthode exceptionnelle ou de la suspendre, selon le cas.
§ 4. En cas d'extrême urgence, et lorsque tout retard apporté à l'autorisation est de nature à compromettre gravement les intérêts visés à	§ 4. En cas d'extrême urgence, et lorsque tout retard apporté à l'autorisation est de nature à compromettre gravement les intérêts visés à

l'article 18/9, le dirigeant du service peut autoriser verbalement la méthode exceptionnelle de recueil de données pour une durée ne pouvant excéder cinq jours, après avoir obtenu au bénéfice de l'urgence l'avis conforme verbal du président de la Commission.	l'article 18/9, le dirigeant du service peut autoriser verbalement la méthode exceptionnelle de recueil de données pour une durée ne pouvant excéder cinq jours, après avoir obtenu au bénéfice de l'urgence l'avis conforme verbal du président de la Commission.
Si le président de la Commission n'est pas joignable, le dirigeant du service peut prendre contact avec un autre membre de la Commission.	Si le président de la Commission n'est pas joignable, le dirigeant du service peut prendre contact avec un autre membre de la Commission.
Le président, ou l'autre membre contacté, informe immédiatement les autres membres de la Commission de son avis verbal.	Le président, ou l'autre membre contacté, informe immédiatement les autres membres de la Commission de son avis verbal.
L'officier de renseignement peut requérir par écrit le concours des personnes visées aux articles 18/14, 18/15, 18/16 et 18/17. La nature de la méthode leur est communiquée. Cette réquisition est communiquée le plus rapidement possible au dirigeant du service.	L'officier **des méthodes** ~~de renseignement~~ peut requérir par écrit le concours des personnes visées aux articles 18/14, 18/15, 18/16 et 18/17. La nature de la méthode leur est communiquée. Cette réquisition est communiquée le plus rapidement possible au dirigeant du service.
Le dirigeant du service confirme par écrit l'autorisation verbale et la notifie au siège de la Commission, selon les modalités fixées par le Roi, au maximum dans les vingt-quatre heures de cette autorisation. Cette confirmation écrite comprend les mentions visées au paragraphe 2.	Le dirigeant du service confirme par écrit l'autorisation verbale et la notifie au siège de la Commission, selon les modalités fixées par le Roi, au maximum dans les vingt-quatre heures de cette autorisation. Cette confirmation écrite comprend les mentions visées au paragraphe 2.
Le cas échéant, cette confirmation indique les motifs qui justifient le maintien de la mise en œuvre de la méthode au-delà du délai de cinq jours, sans excéder les deux mois visés au paragraphe 1er, alinéa 2. Dans ce cas, cette confirmation vaut projet d'autorisation visé au paragraphe 1er.	Le cas échéant, cette confirmation indique les motifs qui justifient le maintien de la mise en œuvre de la méthode au-delà du délai de cinq jours, sans excéder les deux mois visés au paragraphe 1er, alinéa 2. Dans ce cas, cette confirmation vaut projet d'autorisation visé au paragraphe 1er.
Dans le cas où la nécessité du maintien de la méthode au-delà du délai de cinq jours n'a pas pu être anticipée ou dans des circonstances exceptionnelles, le dirigeant du service peut en	Dans le cas où la nécessité du maintien de la méthode au-delà du délai de cinq jours n'a pas pu être anticipée ou dans des circonstances exceptionnelles, le dirigeant du service peut en

autoriser la prolongation selon la procédure de l'alinéa 1er.	autoriser la prolongation selon la procédure de l'alinéa 1er.
Si le président rend un avis verbal négatif, la méthode exceptionnelle de recueil de données ne peut pas être mise en œuvre par le service concerné.	Si le président **ou le membre de la Commission contacté** rend un avis verbal négatif, la méthode exceptionnelle de recueil de données ne peut pas être mise en œuvre par le service concerné.
Si le président ne rend pas immédiatement un avis dans les cas d'extrême urgence, le service concerné peut saisir le ministre compétent, qui autorisera ou non le recours à la méthode envisagée. Le ministre communique sa décision aux présidents de la commission et du Comité permanent R.	Si le président **ou le membre de la Commission contacté** ne rend pas immédiatement un avis dans les cas d'extrême urgence, le service concerné peut saisir le ministre compétent, qui autorisera ou non le recours à la méthode envisagée. Le ministre communique sa décision aux présidents de la commission et du Comité permanent R.
Le dirigeant du service informe le ministre du suivi de la méthode exceptionnelle ainsi autorisée en lui faisant, selon une périodicité fixée par le ministre dans son autorisation, un rapport circonstancié sur le déroulement de la méthode.	Le dirigeant du service informe le ministre du suivi de la méthode exceptionnelle ainsi autorisée en lui faisant, selon une périodicité fixée par le ministre dans son autorisation, un rapport circonstancié sur le déroulement de la méthode.
Le ministre concerné met fin à la méthode exceptionnelle qu'il a autorisée lorsque la menace potentielle qui la justifie a disparu ou si la méthode en question ne s'avère plus utile à la finalité pour laquelle elle a été décidée. Il suspend la méthode lorsqu'il constate une illégalité. Dans ce cas, le ministre concerné porte sans délai à la connaissance de la commission, du dirigeant du service et du Comité permanent R sa décision motivée de mettre fin à la méthode ou de la suspendre, selon le cas.	Le ministre concerné met fin à la méthode exceptionnelle qu'il a autorisée lorsque la menace potentielle qui la justifie a disparu ou si la méthode en question ne s'avère plus utile à la finalité pour laquelle elle a été décidée. Il suspend la méthode lorsqu'il constate une illégalité. Dans ce cas, le ministre concerné porte sans délai à la connaissance de la commission, du dirigeant du service et du Comité permanent R sa décision motivée de mettre fin à la méthode ou de la suspendre, selon le cas.
Il est en tout cas mis fin à la méthode exceptionnelle dans les cinq jours à compter de l'autorisation accordée par le ministre concerné, sauf dans les cas de prolongation visés aux alinéas 5 et 6.	Il est en tout cas mis fin à la méthode exceptionnelle dans les cinq jours à compter de l'autorisation accordée par le ministre concerné, sauf dans les cas de prolongation visés aux alinéas 5 et 6.
§ 5. Le dirigeant du service peut, sur avis conforme préalable de la commission, autoriser la prolongation de la méthode	§ 5. Le dirigeant du service peut, sur avis conforme préalable de la commission, autoriser la prolongation de la méthode exceptionnelle de

exceptionnelle de recueil de données pour une nouvelle période ne pouvant excéder deux mois à compter de l'échéance de la méthode en cours, sans préjudice de l'obligation qui lui est faite de mettre fin à la méthode dès que la menace potentielle qui la justifie a disparu que la méthode n'est plus utile à la finalité pour laquelle elle a été décidée ou qu'il constate une illégalité. Dans ce cas, le dirigeant du service concerné porte à la connaissance de la commission sa décision motivée de mettre fin à la méthode exceptionnelle.	recueil de données pour une nouvelle période ne pouvant excéder deux mois à compter de l'échéance de la méthode en cours, sans préjudice de l'obligation qui lui est faite de mettre fin à la méthode dès que la menace potentielle qui la justifie a disparu que la méthode n'est plus utile à la finalité pour laquelle elle a été décidée ou qu'il constate une illégalité. Dans ce cas, le dirigeant du service concerné porte à la connaissance de la commission sa décision motivée de mettre fin à la méthode exceptionnelle.
Une seconde prolongation et toute nouvelle prolongation de la méthode exceptionnelle de recueil de données n'est possible qu'en présence de circonstances particulières nécessitant de prolonger l'utilisation de cette méthode. Ces motifs particuliers sont indiqués dans la décision. Si ces circonstances particulières font défaut, il doit être mis fin à la méthode.	Une seconde prolongation et toute nouvelle prolongation de la méthode exceptionnelle de recueil de données n'est possible qu'en présence de circonstances particulières nécessitant de prolonger l'utilisation de cette méthode. Ces motifs particuliers sont indiqués dans la décision. Si ces circonstances particulières font défaut, il doit être mis fin à la méthode.
Les conditions prévues aux paragraphes 1er à 3 sont applicables aux modalités de prolongation de la méthode exceptionnelle de recueil de données qui sont prévues dans le présent paragraphe.	Les conditions prévues aux paragraphes 1er à 3 sont applicables aux modalités de prolongation de la méthode exceptionnelle de recueil de données qui sont prévues dans le présent paragraphe.
§ 6. Les membres de la commission peuvent à tout moment contrôler la légalité des méthodes exceptionnelles de recueil de données, y compris le respect des principes de subsidiarité et de proportionnalité, prévues à l'article 18/9, § § 2 et 3.	§ 6. Les membres de la commission peuvent à tout moment contrôler la légalité des méthodes exceptionnelles de recueil de données, y compris le respect des principes de subsidiarité et de proportionnalité, prévues à l'article 18/9, § § 2 et 3.
Ils peuvent à cet effet pénétrer dans les lieux où sont réceptionnées ou conservées les données recueillies par ces méthodes exceptionnelles, se saisir de toutes les pièces utiles et entendre les membres du service.	Ils peuvent à cet effet pénétrer dans les lieux où sont réceptionnées ou conservées les données recueillies par ces méthodes exceptionnelles, se saisir de toutes les pièces utiles et entendre les membres du service.
La commission met fin à la méthode exceptionnelle de recueil de données	La commission met fin à la méthode exceptionnelle de recueil de données lorsqu'elle

lorsqu'elle constate que la menace potentielle qui la justifie a disparu ou si la méthode exceptionnelle ne s'avère plus utile à la finalité pour laquelle elle a été mise en œuvre, ou suspend la méthode exceptionnelle en cas d'illégalité.	constate que la menace potentielle qui la justifie a disparu ou si la méthode exceptionnelle ne s'avère plus utile à la finalité pour laquelle elle a été mise en œuvre, ou suspend la méthode exceptionnelle en cas d'illégalité.
Les données recueillies dans des conditions qui ne respectent pas les dispositions légales en vigueur sont conservées sous le contrôle de la commission, selon les modalités et délais fixés par le Roi, après avis de la commission de la protection de la vie privée. La commission interdit aux services de renseignement et de sécurité d'exploiter ces données.	Les données recueillies dans des conditions qui ne respectent pas les dispositions légales en vigueur sont conservées sous le contrôle de la commission, selon les modalités et délais fixés par le Roi, après avis ~~de la commission de la protection de la vie privée~~ **du Comité permanent R**. La commission interdit aux services de renseignement et de sécurité d'exploiter ces données.
§ 7. La commission informe, de sa propre initiative, le Comité permanent R du projet d'autorisation, visé au paragraphe 2, introduit par le service de renseignement et de sécurité concerné, de l'avis conforme visé au § 3, la confirmation écrite de l'autorisation verbale visée au paragraphe 4, de l'éventuelle prolongation, visée au § 5, de la méthode exceptionnelle de recueil de données et de sa décision visée au § 6 de mettre fin à la méthode ou, le cas échéant, de la suspendre et d'interdire l'exploitation des données ainsi recueillies.	§ 7. La commission informe, de sa propre initiative, le Comité permanent R du projet d'autorisation, visé au paragraphe 2, introduit par le service de renseignement et de sécurité concerné, de l'avis conforme visé au § 3, la confirmation écrite de l'autorisation verbale visée au paragraphe 4, de l'éventuelle prolongation, visée au § 5, de la méthode exceptionnelle de recueil de données et de sa décision visée au § 6 de mettre fin à la méthode ou, le cas échéant, de la suspendre et d'interdire l'exploitation des données ainsi recueillies.
Art. 18/12/1	**Art. 18/12/1**
	Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, s'infiltrer dans le monde réel, conformément aux directives du Conseil national de sécurité.
	Le monde réel vise les relations qui se déroulent principalement avec des contacts physiques directs sans dissimuler son apparence physique.
	La méthode est autorisée aussi longtemps qu'elle est nécessaire aux finalités pour lesquelles elle est mise en œuvre.

	Le service de renseignement et de sécurité concerné fait rapport à la Commission tous les deux mois sur l'évolution de la menace qui a nécessité le recours à l'infiltration dans le monde réel. Ce rapport met en évidence les éléments qui justifient soit le maintien de la méthode exceptionnelle, soit la fin de celle-ci.
Art. 18/15	**Art. 18/15**
§ 1er. Dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité peuvent requérir les renseignements suivants :	**§1. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir des informations relatives aux produits, services et transactions de nature financière et aux valeurs virtuelles, concernant la personne visée, auprès:**
1° la liste des comptes bancaires, des coffres bancaires ou des instruments financiers définis à l'article 2, 1°, de la loi du 2 août 2002 relative à la surveillance du secteur financiers, et aux services financiers dont la personne visée est le titulaire, le mandataire ou le véritable bénéficiaire, et, le cas échéant, toutes les données à ce sujet;	**1° des personnes et institutions visées à l'article 5, paragraphe 1er, 3° à 22° de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces ;**
2° les transactions bancaires qui ont été réalisées, pendant une période déterminée, sur un ou plusieurs de ces comptes bancaires ou instruments financiers, y compris les informations concernant tout compte émetteur ou récepteur;	**2° des personnes et institutions qui, sur le territoire belge, mettent à disposition ou proposent des services en lien avec des valeurs virtuelles permettant d'échanger des moyens de paiement réglementés en valeurs virtuelles ;**
3° les données concernant les titulaires ou mandataires qui, pendant une période déterminée, ont ou avaient accès à ces coffres bancaires.	**3° du Point de Contact Central tenu par la Banque nationale de Belgique conformément à la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt.**
§ 2. L'organisme bancaire ou l'institution financière est tenu de remettre sans délai les	**§ 2. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs**

informations sollicitées à un agent du service désigné à cet effet par le dirigeant du service, sur présentation de sa carte de légitimation et d'une demande écrite du dirigeant du service. Cette demande mentionne la nature de l'avis conforme de la commission, la nature de l'avis conforme du président de la commission ou la nature de l'autorisation du ministre concerné, selon le cas.	**missions, exiger des personnes et institutions visées au paragraphe 1er, 1° et 2° le placement sous surveillance des transactions de la personne visée.**
L'organisme bancaire ou l'institution financière qui refuse de prêter le concours visé au présent article est puni d'une amende de vingt-six euros à vingt mille euros.	**§ 3. La coopération requise visée au paragraphe premier, 3° a lieu conformément à la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt.**
	La personne ou l'institution requise, visée au paragraphe premier, 1° et 2°, est tenue de remettre sans délai les informations demandées après réception de la réquisition écrite du dirigeant du service.
	Cette réquisition mentionne, selon le cas, la nature de l'avis conforme de la Commission, la nature de l'avis conforme du président de la Commission ou la nature de l'autorisation du ministre concerné. Dans la réquisition, le service de renseignement et de sécurité concerné fournit également une description précise des informations requises et détermine la forme sous laquelle elles doivent être communiquées.
	§ 4. Toute personne ou institution requise qui refuse de communiquer les données ou qui ne les communique pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition est punie d'un emprisonnement de huit jours à un an et d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement.
Art. 20.	**Art. 20.**

§ 1er. Les services de renseignement et de sécurité, les services de police, les autorités administratives et judiciaires veillent à assurer entre eux une coopération mutuelle aussi efficace que possible. Les services de renseignement et de sécurité veillent également à assurer une collaboration avec les services de renseignement et de sécurité étrangers.	§ 1er. Les services de renseignement et de sécurité, les services de police, les autorités administratives et judiciaires veillent à assurer entre eux une coopération mutuelle aussi efficace que possible. Les services de renseignement et de sécurité veillent également à assurer une ~~collaboration~~ **coopération** avec les services de renseignement et de sécurité étrangers.
§ 2. Lorsqu'ils en sont sollicités par celles-ci, les services de renseignement et de sécurité peuvent, dans les limites d'un protocole approuvé par les ministres concernés, prêter leur concours et notamment leur assistance technique aux autorités judiciaires et administratives.	§ 2. Lorsqu'ils en sont sollicités par celles-ci, les services de renseignement et de sécurité peuvent~~, dans les limites d'un protocole approuvé par les ministres concernés,~~ prêter leur concours et notamment leur assistance technique aux autorités judiciaires et administratives.
	Les modalités de ce concours peuvent être déterminées dans le cadre d'un protocole.
§ 3. Le Conseil national de sécurité définit les conditions de la communication prévue à l'article 19, alinéa 1er, et de la coopération prévue au § 1er du présent article.	§ 3. Le Conseil national de sécurité définit les conditions de la communication prévue à l'article 19, alinéa 1er, et de la coopération prévue au § 1er du présent article.
§ 4. Pour les missions décrites à l'article 7, 3°/1 et à l'article 11, § 1er, 5°, la Sûreté de l'Etat et le Service Général du Renseignement et de la Sécurité concluent un accord de coopération sur la base de directives obtenues du Conseil national de sécurité.	§ 4. Pour les missions décrites à l'article 7, 3°/1 et à l'article 11, § 1er, 5°, la Sûreté de l'Etat et le Service Général du Renseignement et de la Sécurité concluent un accord de coopération sur la base de directives obtenues du Conseil national de sécurité.

COÖRDINATIE VAN DE ARTIKELEN

BASISTEKST	BASISTEKST AANGEPAST AAN HET WETSONTWERP
Art. 3.	**Art. 3.**
In deze wet wordt verstaan onder :	In deze wet wordt verstaan onder :
1° "Nationale Veiligheidsraad": de binnen de Regering opgerichte Raad die belast is met de door de Koning vastgestelde taken van nationale veiligheid;	1° "Nationale Veiligheidsraad": de binnen de Regering opgerichte Raad die belast is met de door de Koning vastgestelde taken van nationale veiligheid;
2° "agent" : ieder lid van het statutair of contractueel personeel en iedere militair die zijn functie uitoefent binnen één van de in artikel 2 genoemde inlichtingen- en veiligheidsdiensten;	2° "agent" : ieder lid van het statutair of contractueel personeel en iedere militair die zijn functie uitoefent binnen één van de in artikel 2 genoemde inlichtingen- en veiligheidsdiensten;
3° "lid van het interventieteam":	3° "lid van het interventieteam":
a) voor de Veiligheid van de Staat, de agent bedoeld in de artikelen 22 tot 35 die belast is met de bescherming van het personeel, de infrastructuur en de goederen van de Veiligheid van de Staat;	a) voor de Veiligheid van de Staat, de agent bedoeld in de artikelen 22 tot 35 die belast is met de bescherming van het personeel, de infrastructuur en de goederen van de Veiligheid van de Staat;
b) voor de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht, de agent bedoeld in de artikelen 22 tot 35 die belast is met de bescherming van het personeel, de infrastructuur en de goederen van de Algemene Dienst Inlichting en Veiligheid;	b) voor de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht, de agent bedoeld in de artikelen 22 tot 35 die belast is met de bescherming van het personeel, de infrastructuur en de goederen van de Algemene Dienst Inlichting en Veiligheid;
4° "Algemene Dienst Inlichting en Veiligheid" : de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht.	4° "Algemene Dienst Inlichting en Veiligheid" : de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht.
5° " de Minister " : de Minister van Justitie voor wat de Veiligheid van de Staat betreft, en de Minister van Landsverdediging voor wat de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht betreft;	5° " de Minister " : de Minister van Justitie voor wat de Veiligheid van de Staat betreft, en de Minister van Landsverdediging voor wat de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht betreft;
6° " de commissie " : de bestuurlijke commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en	6° " de **Commissie** " : de bestuurlijke commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en

veiligheidsdiensten, die wordt opgericht bij artikel 43/1;	veiligheidsdiensten, die wordt opgericht bij artikel 43/1;
7° " het Vast Comité I " : het Vast Comité van Toezicht op de inlichtingendiensten, zoals bedoeld in de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;	7° " het Vast Comité I " : het Vast Comité van Toezicht op de inlichtingendiensten, zoals bedoeld in de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;
8° " het diensthoofd " : enerzijds, de administrateur-generaal van de Veiligheid van de Staat of, bij verhindering, de dienstdoende administrateur-generaal, en anderzijds, het hoofd van de algemene Dienst inlichting en veiligheid van de Krijgsmacht of, bij verhindering, het dienstdoende hoofd;	8° " het diensthoofd " : enerzijds, de administrateur-generaal van de Veiligheid van de Staat of, bij verhindering, de dienstdoende administrateur-generaal, en anderzijds, het hoofd van de algemene Dienst inlichting en veiligheid van de Krijgsmacht of, bij verhindering, het dienstdoende hoofd;
	8°/1 "zijn gedelegeerde": de agent, andere dan de dossierbeheerder, aangesteld door middel van een schriftelijke beslissing van het diensthoofd die overgemaakt werd aan het Vast Comité I, om gewoonlijk bepaalde beslissingen in de plaats van het diensthoofd te nemen;
9° "de inlichtingenofficier":	9° "**de methodenofficier** ":
a) voor de Veiligheid van de Staat, de agent die ten minste de graad van commissaris heeft;	a) voor de Veiligheid van de Staat, de agent die ten minste de graad van commissaris heeft;
b) voor de Algemene Dienst Inlichting en Veiligheid, de aan deze dienst toegewezen officier, alsook de burgerambtenaar die ten minste de graad van commissaris heeft;	b) voor de Algemene Dienst Inlichting en Veiligheid, de aan deze dienst toegewezen officier, alsook de burgerambtenaar die ten minste de graad van commissaris heeft;
10° " communicatie " : elke overbrenging, uitzending, of ontvangst van tekens, seinen, geschriften, beelden, klanken of gegevens van alle aard, per draad, radio-elektriciteit, optische seingeving of een ander elektromagnetisch systeem; de communicatie per telefoon, gsm, mobilofoon, telex, telefax of elektronische gegevensoverdracht via computer of computernetwerk, evenals iedere andere privécommunicatie;	10° " communicatie " : elke overbrenging, uitzending, of ontvangst van tekens, seinen, geschriften, beelden, klanken of gegevens van alle aard, per draad, radio-elektriciteit, optische seingeving of een ander elektromagnetisch systeem; de communicatie per telefoon, gsm, mobilofoon, telex, telefax of elektronische gegevensoverdracht via computer of computernetwerk, evenals iedere andere privécommunicatie;
11° " elektronische communicatienetwerken " : de elektronische communicatienetwerken als bedoeld in artikel 2, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;	11° " elektronische communicatienetwerken " : de elektronische communicatienetwerken als bedoeld in artikel 2, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

11° /1 "verstrekker van een elektronische communicatiedienst": iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen, te ontvangen of te verspreiden;	11° /1 "verstrekker van een elektronische communicatiedienst": iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen, te ontvangen of te verspreiden;
12° "voor het publiek toegankelijke plaats": elke plaats, openbaar of privé, waartoe het publiek toegang kan hebben;	12° "voor het publiek toegankelijke plaats": elke plaats, openbaar of privé, waartoe het publiek toegang kan hebben;
12° /1 "niet voor het publiek toegankelijke plaats die niet aan het zicht onttrokken is": elke plaats waartoe het publiek geen toegang heeft en die voor iedereen zichtbaar is vanaf de openbare weg zonder hulpmiddel of kunstgreep, met uitzondering van de binnenkant van gebouwen die niet voor het publiek toegankelijk zijn;	12° /1 "niet voor het publiek toegankelijke plaats die niet aan het zicht onttrokken is": elke plaats waartoe het publiek geen toegang heeft en die voor iedereen zichtbaar is vanaf de openbare weg zonder hulpmiddel of kunstgreep, met uitzondering van de binnenkant van gebouwen die niet voor het publiek toegankelijk zijn;
13° " post " : de postzending zoals gedefinieerd in artikel 131, 6°, 7° en 11°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;	13° " post " : de postzending zoals gedefinieerd in artikel 131, 6°, 7° en 11°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;
14° " technisch middel " : een configuratie van componenten die signalen detecteert, deze overbrengt, hun registratie activeert en de signalen registreert, met uitzondering van:	14° " technisch middel " : een configuratie van componenten die signalen detecteert, deze overbrengt, hun registratie activeert en de signalen registreert, met uitzondering van:
a) een apparaat dat gebruikt wordt voor het nemen van foto's;	a) een apparaat dat gebruikt wordt voor het nemen van foto's;
b) een mobiel apparaat dat gebruikt wordt voor de opname van bewegende beelden indien het nemen van foto's de discretie en de veiligheid van de agenten niet kan verzekeren en op voorwaarde dat dit gebruik voorafgaand is toegestaan door het diensthoofd of zijn gedelegeerde. Enkel relevant geachte vaste beelden worden bewaard. De overige beelden worden vernietigd binnen een maand na de dag van de opname;	b) een mobiel apparaat dat gebruikt wordt voor de opname van bewegende beelden indien het nemen van foto's de discretie en de veiligheid van de agenten niet kan verzekeren en op voorwaarde dat dit gebruik voorafgaand is toegestaan door het diensthoofd of zijn gedelegeerde. Enkel relevant geachte vaste beelden worden bewaard. De overige beelden worden vernietigd binnen een maand na de dag van de opname;
15° " radicaliseringsproces " : een proces waarbij een individu of een groep van individuen op dusdanige wijze wordt beïnvloed	15° " radicaliseringsproces " : een proces waarbij een individu of een groep van individuen op dusdanige wijze wordt beïnvloed dat dit individu

dat dit individu of deze groep van individuen mentaal gevormd wordt of bereid is tot het plegen van terroristische handelingen;	of deze groep van individuen mentaal gevormd wordt of bereid is tot het plegen van terroristische handelingen;
16° " journalist " : een journalist die gerechtigd is de titel van beroepsjournalist te dragen overeenkomstig de wet van 30 december 1963 betreffende de erkenning en de bescherming van de titel van beroepsjournalist;	16° " journalist " : een journalist die gerechtigd is de titel van beroepsjournalist te dragen overeenkomstig de wet van 30 december 1963 betreffende de erkenning en de bescherming van de titel van beroepsjournalist;
17° " bronnengeheim " : het geheim zoals omschreven in de wet van 7 april 2005 tot bescherming van de journalistieke bronnen;	17° " bronnengeheim " : het geheim zoals omschreven in de wet van 7 april 2005 tot bescherming van de journalistieke bronnen;
18° " Directeur Operaties van de Veiligheid van de Staat " : de agent van de buitendiensten van de Veiligheid van de Staat, bekleed met de graad van commissaris-generaal, die belast is met de leiding van de buitendiensten van de Veiligheid van de Staat;	18° " Directeur Operaties van de Veiligheid van de Staat " : de agent van de buitendiensten van de Veiligheid van de Staat, bekleed met de graad van commissaris-generaal, die belast is met de leiding van de buitendiensten van de Veiligheid van de Staat;
19° "vergrendeld voorwerp": een voorwerp dat geopend moet worden met behulp van een valse sleutel of via braak;	19° "vergrendeld voorwerp": een voorwerp dat geopend moet worden met behulp van een valse sleutel of via braak;
20° "observatie": het waarnemen van één of meerdere personen, hun aanwezigheid of gedrag, of van zaken, plaatsen of gebeurtenissen;	20° "observatie": het waarnemen van één of meerdere personen, hun aanwezigheid of gedrag, of van zaken, plaatsen of gebeurtenissen;
21° "doorzoeking": het betreden, bezichtigen en onderzoeken van een plaats alsook het bezichtigen en onderzoeken van een voorwerp.	21° "doorzoeking": het betreden, bezichtigen en onderzoeken van een plaats alsook het bezichtigen en onderzoeken van een voorwerp;
	22° “valse naam”: een naam die niet toebehoort aan de agent en die niet wordt aangetoond door middel van een identiteitskaart, een paspoort, een vreemdelingenkaart of een verblijfsdocument of door officiële documenten die hieruit voortvloeien;
	23° “valse hoedanigheid”: een hoedanigheid die niet toekomt aan de agent en waaruit geen rechtsgevolg voortvloeit;
	24° "fictieve identiteit": een valse identiteit, die wordt aangetoond door middel van een identiteitskaart, een paspoort, een vreemdelingenkaart of een verblijfsdocument;

	25° "fictieve hoedanigheid": een statuut, een titel of een functie die niet toebehoort aan de agent en waaruit rechtsgevolgen voortvloeien;
	26° "menselijke bron": een persoon die een inlichting meedeelt aan de inlichtingen- en veiligheidsdiensten en die geregistreerd is overeenkomstig de procedure beschreven in de door de Nationale Veiligheidsraad goedgekeurde richtlijn betreffende het beroep op menselijke bronnen;
	27° "infiltreren": de handeling waarbij een agent, buiten de gevallen bedoeld in artikel 18, zich doelbewust in een groep of in het leven van een persoon integreert om informatie of gegevens te verzamelen in het kader van een onderzoek van een inlichtingen- en veiligheidsdienst en in het belang van de uitoefening van zijn opdrachten, hetzij in de virtuele wereld, hetzij in de reële wereld. Deze agent verbergt zijn hoedanigheid van agent van de inlichtingen- en veiligheidsdiensten en, voor de agenten van de Algemene Dienst Inlichting en Veiligheid, van lid van het ministerie van Defensie, en :
	a) neemt deel aan de activiteiten of faciliteert deze of ondersteunt actief de overtuigingen of de activiteiten van de persoon of de groep die het voorwerp uitmaakt van het onderzoek, of
	b) onderhoudt duurzame contacten met hen.
Art. 11.	**Art. 11.**
§ 1. De Algemene Dienst Inlichting en Veiligheid heeft als opdracht:	§ 1. De Algemene Dienst Inlichting en Veiligheid heeft als opdracht:
1° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de factoren die de nationale en internationale veiligheid beïnvloeden of kunnen beïnvloeden in die mate dat de Krijgsmacht betrokken is of zou kunnen worden om inlichtingensteun te bieden aan hun lopende of eventuele komende operaties, alsook de inlichtingen die betrekking hebben op elke activiteit die:	1° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de factoren die de nationale en internationale veiligheid beïnvloeden of kunnen beïnvloeden in die mate dat de Krijgsmacht betrokken is of zou kunnen worden om inlichtingensteun te bieden aan hun lopende of eventuele komende operaties, alsook de inlichtingen die betrekking hebben op elke activiteit die:
a) de onschendbaarheid van het nationaal grondgebied of de bevolking,	a) de onschendbaarheid van het nationaal grondgebied of de bevolking,

b) de militaire defensieplannen,	b) de militaire defensieplannen,
c) het wetenschappelijk en economisch potentieel met betrekking tot de actoren, zowel de natuurlijke als de rechtspersonen, die actief zijn in de economische en industriële sectoren die verbonden zijn met defensie en die opgenomen zijn in een op voorstel van de minister van Justitie en de minister van Landsverdediging door de Nationale Veiligheidsraad goedgekeurde lijst,	c) het wetenschappelijk en economisch potentieel met betrekking tot de actoren, zowel de natuurlijke als de rechtspersonen, die actief zijn in de economische en industriële sectoren die verbonden zijn met defensie en die opgenomen zijn in een op voorstel van de minister van Justitie en de minister van Landsverdediging door de Nationale Veiligheidsraad goedgekeurde lijst,
d) de vervulling van de opdrachten van de strijdkrachten,	d) de vervulling van de opdrachten van de strijdkrachten,
e) de veiligheid van de Belgische onderdanen in het buitenland,	e) de veiligheid van de Belgische onderdanen in het buitenland,
f) elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van de Nationale Veiligheidsraad, bedreigt of zou kunnen bedreigen;	f) elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van de Nationale Veiligheidsraad,
	bedreigt of zou kunnen bedreigen;
en er de bevoegde ministers onverwijld over inlichten alsook de regering, op haar verzoek, advies te verlenen bij de omschrijving van haar binnen- en buitenlands beleid inzake veiligheid en defensie;	en er de bevoegde ministers onverwijld over inlichten alsook de regering, op haar verzoek, advies te verlenen bij de omschrijving van haar binnen- en buitenlands beleid inzake veiligheid en defensie;
2° het zorgen voor het behoud van de militaire veiligheid van het personeel dat onder de Minister van Landsverdediging ressorteert, de militaire installaties, wapens en wapensystemen, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen en, in het kader van de cyberaanvallen op wapensystemen, militaire informatica- en verbindingssystemen of systemen die de Minister van Landsverdediging beheerst, de aanval neutraliseren en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het recht van de gewapende conflicten;	2° het zorgen voor het behoud van de militaire veiligheid van het personeel dat onder de Minister van Landsverdediging ressorteert, de militaire installaties, wapens en wapensystemen, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen en, in het kader van de cyberaanvallen op wapensystemen, militaire informatica- en verbindingssystemen of systemen die de Minister van Landsverdediging **beheert**, de aanval neutraliseren en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het **internationaal recht**;
	2°/1 het neutraliseren, in het kader van een nationale cybersecurity crisis, van een

	cyberaanval op informatica- en verbindingssystemen niet beheerd door de Minister van Landsverdediging en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het internationaal recht;
3° het beschermen van het geheim dat, krachtens de internationale verbintenissen van België of teneinde de onschendbaarheid van het nationaal grondgebied en de vervulling van de opdrachten van de strijdkrachten te verzekeren, verbonden is met de militaire installaties, wapens, munitie, uitrusting, met de plannen, geschriften, documenten of andere militaire voorwerpen, met de militaire inlichtingen en verbindingen, alsook met de militaire informatica- en verbindingssystemen of die systemen die de Minister van Landsverdediging beheert;	3° het beschermen van het geheim dat, krachtens de internationale verbintenissen van België of teneinde de onschendbaarheid van het nationaal grondgebied en de vervulling van de opdrachten van de strijdkrachten te verzekeren, verbonden is met de militaire installaties, wapens, munitie, uitrusting, met de plannen, geschriften, documenten of andere militaire voorwerpen, met de militaire inlichtingen en verbindingen, alsook met de militaire informatica- en verbindingssystemen of die systemen die de Minister van Landsverdediging beheert;
4° het uitvoeren van de veiligheidsonderzoeken die hem overeenkomstig de richtlijnen van de Nationale Veiligheidsraad worden toevertrouwd.	4° het uitvoeren van de veiligheidsonderzoeken die hem overeenkomstig de richtlijnen van de Nationale Veiligheidsraad worden toevertrouwd**;**
5° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied.	5° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied**;**
	6° het uitvoeren van alle andere opdrachten die hem door of krachtens de wet worden toevertrouwd.
§ 2. Voor de toepassing van § 1 wordt verstaan onder :	§ 2. Voor de toepassing van § 1 wordt verstaan onder :
1° "activiteit die de onschendbaarheid van het nationaal grondgebied of de bevolking bedreigt of zou kunnen bedreigen" : elke uiting van het voornemen om, met middelen van militaire aard, het gehele grondgebied of een gedeelte ervan, alsook het luchtruim boven dat grondgebied of de territoriale wateren, in te nemen, te bezetten of aan te vallen, of de bescherming of het voortbestaan van de gehele bevolking of een gedeelte ervan, het nationaal patrimonium of het economisch potentieel van het land in gevaar te brengen;	1° "activiteit die de onschendbaarheid van het nationaal grondgebied of de bevolking bedreigt of zou kunnen bedreigen" : elke uiting van het voornemen om, met middelen van militaire aard, het gehele grondgebied of een gedeelte ervan, alsook het luchtruim boven dat grondgebied of de territoriale wateren, in te nemen, te bezetten of aan te vallen, of de bescherming of het voortbestaan van de gehele bevolking of een gedeelte ervan, het nationaal patrimonium of het economisch potentieel van het land in gevaar te brengen;

2° "activiteit die de militaire defensieplannen bedreigt of zou kunnen bedreigen" : elke uiting van het voornemen om op ongeoorloofde wijze kennis te nemen van de plannen betreffende de militaire verdediging van het nationaal grondgebied, van het luchtruim boven dat grondgebied of van de territoriale wateren en van de vitale belangen van de Staat, of betreffende de gemeenschappelijke militaire verdediging in het kader van een bondgenootschap of een internationaal of supranationaal samenwerkingsverband;	2° "activiteit die de militaire defensieplannen bedreigt of zou kunnen bedreigen" : elke uiting van het voornemen om op ongeoorloofde wijze kennis te nemen van de plannen betreffende de militaire verdediging van het nationaal grondgebied, van het luchtruim boven dat grondgebied of van de territoriale wateren en van de vitale belangen van de Staat, of betreffende de gemeenschappelijke militaire verdediging in het kader van een bondgenootschap of een internationaal of supranationaal samenwerkingsverband;
2°/1 " activiteit die het wetenschappelijk en economisch potentieel bedreigt of zou kunnen bedreigen met betrekking tot de actoren, zowel de natuurlijke als de rechtspersonen, die actief zijn in de economische en industriële sectoren en die opgenomen zijn in een op voorstel van de Minister van Justitie en de Minister van Landsverdediging door de Nationale Veiligheidsraad goedgekeurde lijst " : elke uiting van het voornemen om de essentiële elementen van het wetenschappelijk en economisch potentieel van deze actoren in het gedrang te brengen;	2°/1 " activiteit die het wetenschappelijk en economisch potentieel bedreigt of zou kunnen bedreigen met betrekking tot de actoren, zowel de natuurlijke als de rechtspersonen, die actief zijn in de economische en industriële sectoren en die opgenomen zijn in een op voorstel van de Minister van Justitie en de Minister van Landsverdediging door de Nationale Veiligheidsraad goedgekeurde lijst " : elke uiting van het voornemen om de essentiële elementen van het wetenschappelijk en economisch potentieel van deze actoren in het gedrang te brengen;
3° "activiteit die de vervulling van de opdrachten van de strijdkrachten bedreigt of zou kunnen bedreigen" : elke uiting van het voornemen om de paraatstelling, de mobilisatie en de aanwending van de Belgische Krijgsmacht, van de geallieerde strijdkrachten of van intergeallieerde defensie-organisaties te neutraliseren, te belemmeren, te saboteren, in het gedrang te brengen of te verhinderen bij opdrachten, acties of operaties in nationaal verband, in het kader van een bondgenootschap of een internationaal of supranationaal samenwerkingsverband;	3° "activiteit die de vervulling van de opdrachten van de strijdkrachten bedreigt of zou kunnen bedreigen" : elke uiting van het voornemen om de paraatstelling, de mobilisatie en de aanwending van de Belgische Krijgsmacht, van de geallieerde strijdkrachten of van intergeallieerde defensie-organisaties te neutraliseren, te belemmeren, te saboteren, in het gedrang te brengen of te verhinderen bij opdrachten, acties of operaties in nationaal verband, in het kader van een bondgenootschap of een internationaal of supranationaal samenwerkingsverband;
4° "activiteit die de veiligheid van Belgische onderdanen in het buitenland bedreigt of zou kunnen bedreigen" : elke uiting van het voornemen om het leven of de lichamelijke integriteit van Belgen in het buitenland en van hun familieleden collectief te schaden.	4° "activiteit die de veiligheid van Belgische onderdanen in het buitenland bedreigt of zou kunnen bedreigen" : elke uiting van het voornemen om het leven of de lichamelijke integriteit van Belgen in het buitenland en van hun familieleden collectief te schaden.

	5° "nationale cybersecurity crisis": elke cybersecurity gebeurtenis die wegens haar aard of gevolgen:
	- de vitale belangen van het land of de essentiële behoeften van de bevolking bedreigt;
	- een dringende besluitvorming vereist; en
	- de gecoördineerde inzet van verscheidene departementen en organismen vergt.
§ 3. Op verzoek van de Algemene Dienst Inlichting en Veiligheid verleent de Veiligheid van de Staat zijn medewerking bij het inwinnen van inlichtingen wanneer personen die niet ressorteren onder de Minister van Landsverdediging of niet behoren tot ondernemingen die overeenkomsten uitvoeren, welke met hem, met internationale militaire organisaties of met derde landen worden gesloten in militaire aangelegenheden, of die deelnemen aan een gunningsprocedure van een overheidsopdracht die door de laatstgenoemden werd uitgeschreven, betrokken zijn bij activiteiten bedoeld in paragraaf 1, 1°, 2°, 3° en 5°.	§ 3. Op verzoek van de Algemene Dienst Inlichting en Veiligheid verleent de Veiligheid van de Staat zijn medewerking bij het inwinnen van inlichtingen wanneer personen die niet ressorteren onder de Minister van Landsverdediging of niet behoren tot ondernemingen die overeenkomsten uitvoeren, welke met hem, met internationale militaire organisaties of met derde landen worden gesloten in militaire aangelegenheden, of die deelnemen aan een gunningsprocedure van een overheidsopdracht die door de laatstgenoemden werd uitgeschreven, betrokken zijn bij activiteiten bedoeld in **paragraaf 1, 1° tot 3°, 5° en 6°**.
De maatregelen inzake industriële bescherming worden enkel genomen wanneer de Minister van Landsverdediging, derde landen of de organisaties waarmee België verdragsrechtelijk of contractueel verbonden is, hierom verzoeken.	De maatregelen inzake industriële bescherming worden enkel genomen wanneer de Minister van Landsverdediging, derde landen of de organisaties waarmee België verdragsrechtelijk of contractueel verbonden is, hierom verzoeken.
Art. 13.	**Art. 13.**
De inlichtingen- en veiligheidsdiensten kunnen informatie en persoonsgegevens opsporen, verzamelen, ontvangen en verwerken die nuttig kunnen zijn om hun opdrachten te vervullen en een documentatie bijhouden, meer bepaald met betrekking tot de gebeurtenissen, de groeperingen en de personen die een belang vertonen voor de uitoefening van hun opdrachten.	**§1.** De inlichtingen- en veiligheidsdiensten kunnen informatie en persoonsgegevens opsporen, verzamelen, ontvangen en verwerken die nuttig kunnen zijn om hun opdrachten te vervullen en een documentatie bijhouden, meer bepaald met betrekking tot de gebeurtenissen, de groeperingen en de personen die een belang vertonen voor de uitoefening van hun opdrachten.
De in de documentatie vervatte inlichtingen moeten in verband staan met de doeleinden van het gegevensbestand en beperkt blijven tot de vereisten die eruit voortvloeien.	De in de documentatie vervatte inlichtingen moeten in verband staan met de doeleinden van het gegevensbestand en beperkt blijven tot de vereisten die eruit voortvloeien.

De inlichtingen- en veiligheidsdiensten waken over de veiligheid van de gegevens die betrekking hebben op hun bronnen en van de informatie en persoonsgegevens die deze bronnen leveren.	**§2.** De inlichtingen- en veiligheidsdiensten waken over de veiligheid van de gegevens die betrekking hebben op hun bronnen en van de informatie en persoonsgegevens die deze bronnen leveren.
De agenten van de inlichtingen- en veiligheidsdiensten hebben toegang tot de door hun dienst ingewonnen en verwerkte informatie, inlichtingen en persoonsgegevens, voor zover deze nuttig zijn voor de uitoefening van hun functie of opdracht.	**§3.** De agenten van de inlichtingen- en veiligheidsdiensten hebben toegang tot de door hun dienst ingewonnen en verwerkte informatie, inlichtingen en persoonsgegevens, voor zover deze nuttig zijn voor de uitoefening van hun functie of opdracht.
	§4. Indien een agent, tijdens een veiligheidsonderzoek of een veiligheidsverificatie in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, kennis neemt van informatie die wijst op het bestaan van een potentiële dreiging zoals bedoeld in de artikelen 7 en 8 of tegen een belang zoals bedoeld in artikel 11, maakt hij deze onmiddellijk schriftelijk over aan zijn diensthoofd of aan diens gedelegeerde, met het oog op de verwerking ervan ter bestrijding van de voormelde dreiging.
	Onderafdeling 1 – Het plegen van strafbare feiten
Art. 13/1.	**Art. 13/1.**
Het is de agenten verboden strafbare feiten te plegen.	**§1**. Het is de agenten verboden strafbare feiten te plegen.
	§2. In afwijking van paragraaf 1, blijven vrij van straf de agenten die overtredingen, inbreuken op de wegcode of een gebruiksdiefstal begaan die strikt noodzakelijk zijn voor het welslagen van de uitvoering van de opdracht of ter verzekering van hun eigen veiligheid of die van derden, wanneer deze agenten:
	1° belast zijn met de uitvoering van de methoden voor het verzamelen van gegevens; of
	2° leden zijn van het interventieteam.
In afwijking van het eerste lid, blijven vrij van straf de agenten belast met de uitvoering van	~~In afwijking van het eerste lid, blijven vrij van straf de agenten belast met de uitvoering van de~~

de methoden voor het verzamelen van gegevens alsook de leden van het interventieteam in het kader van hun functie, die overtredingen, inbreuken op de wegcode of een gebruiksdiefstal begaan die strikt noodzakelijk zijn voor het welslagen van de uitvoering van de methode of ter verzekering van hun eigen veiligheid of die van andere personen.	~~methoden voor het verzamelen van gegevens alsook de leden van het interventieteam in het kader van hun functie, die overtredingen, inbreuken op de wegcode of een gebruiksdiefstal begaan die strikt noodzakelijk zijn voor het welslagen van de uitvoering van de methode of ter verzekering van hun eigen veiligheid of die van andere personen.~~
Onverminderd het tweede lid, blijven vrij van straf de agenten die bij de uitvoering van de in artikel 18/2 bedoelde methoden, met het voorafgaand schriftelijk akkoord van de Commissie gegeven binnen de vier dagen na ontvangst van de schriftelijke vraag van het diensthoofd, strafbare feiten begaan die strikt noodzakelijk zijn voor het welslagen van de uitvoering van de methode of ter verzekering van hun eigen veiligheid of die van andere personen. In geval van hoogdringendheid vraagt het diensthoofd het voorafgaand mondeling akkoord van de voorzitter van de Commissie. Dit mondelinge akkoord wordt zo spoedig mogelijk schriftelijk bevestigd door de voorzitter van de Commissie. De Commissie of de voorzitter brengt zijn akkoord ter kennis van het Vast Comité I.	~~Onverminderd het tweede lid, blijven vrij van straf de agenten die bij de uitvoering van de in artikel 18/2 bedoelde methoden, met het voorafgaand schriftelijk akkoord van de Commissie gegeven binnen de vier dagen na ontvangst van de schriftelijke vraag van het diensthoofd, strafbare feiten begaan die strikt noodzakelijk zijn voor het welslagen van de uitvoering van de methode of ter verzekering van hun eigen veiligheid of die van andere personen. In geval van hoogdringendheid vraagt het diensthoofd het voorafgaand mondeling akkoord van de voorzitter van de Commissie. Dit mondelinge akkoord wordt zo spoedig mogelijk schriftelijk bevestigd door de voorzitter van de Commissie. De Commissie of de voorzitter brengt zijn akkoord ter kennis van het Vast Comité I.~~
In afwijking van het derde lid, indien de strikte noodzaak om een strafbaar feit te begaan ter verzekering van de veiligheid van agenten of andere personen onmogelijk kon worden voorzien en het evenmin mogelijk was om het voorafgaand akkoord te bekomen van de Commissie of van de voorzitter in geval van een hoogdringendheidsprocedure, brengt het diensthoofd de Commissie zo spoedig mogelijk op de hoogte dat een strafbaar feit werd begaan. Indien de Commissie, na evaluatie, besluit tot de strikte noodzaak en de onvoorzienbaarheid van het strafbaar feit, blijft de agent vrij van straf. De Commissie maakt dit akkoord over aan het Vast Comité I.	~~In afwijking van het derde lid, indien de strikte noodzaak om een strafbaar feit te begaan ter verzekering van de veiligheid van agenten of andere personen onmogelijk kon worden voorzien en het evenmin mogelijk was om het voorafgaand akkoord te bekomen van de Commissie of van de voorzitter in geval van een hoogdringendheidsprocedure, brengt het diensthoofd de Commissie zo spoedig mogelijk op de hoogte dat een strafbaar feit werd begaan. Indien de Commissie, na evaluatie, besluit tot de strikte noodzaak en de onvoorzienbaarheid van het strafbaar feit, blijft de agent vrij van straf. De Commissie maakt dit akkoord over aan het Vast Comité I.~~
De strafbare feiten bedoeld in het tweede tot vierde lid moeten in gelijke verhouding staan tot het door de inlichtingenopdracht nagestreefde doel en mogen in geen geval afbreuk doen aan de fysieke integriteit van personen.	~~De strafbare feiten bedoeld in het tweede tot vierde lid moeten in gelijke verhouding staan tot het door de inlichtingenopdracht nagestreefde doel en mogen in geen geval afbreuk doen aan de fysieke integriteit van personen.~~

Blijven vrij van straf, de leden van de commissie die machtiging verlenen tot het plegen van strafbare feiten zoals bedoeld in het derde en het vierde lid.	~~Blijven vrij van straf, de leden van de commissie die machtiging verlenen tot het plegen van strafbare feiten zoals bedoeld in het derde en het vierde lid.~~
	§3. Onverminderd paragraaf 2, blijven vrij van straf, de agenten die in de uitvoering van de opdrachten bedoeld in de artikelen 7, 1° en 3°/1 en 11, §1, 1° tot 3° en 5°, strafbare feiten plegen die strikt noodzakelijk zijn voor het welslagen van de uitvoering van hun opdracht of ter verzekering van hun eigen veiligheid of die van derden.
	De strafbare feiten, bedoeld in het eerste lid, kunnen slechts worden gepleegd na voorafgaand schriftelijk akkoord van de Commissie. De Commissie geeft haar schriftelijk akkoord binnen de vier dagen na ontvangst van de schriftelijke en gemotiveerde vraag van het diensthoofd.
	Het akkoord geldt voor een maximumtermijn van zes maanden, onverminderd de mogelijkheid om de maatregel te verlengen volgens de procedure bedoeld in het tweede lid.
	De vraag van het diensthoofd vermeldt, op straffe van onwettigheid:
	1° de feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd;
	2° de context van de vraag en de finaliteit;
	3° de lijst met agenten die beantwoorden aan het vereiste profiel om de feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd zoals bedoeld in 1° te plegen;
	4° de strikte noodzakelijkheid;
	5° de proportionaliteit bedoeld in paragraaf 4;
	6° de periode waarbinnen het strafbaar feit of de strafbare feiten kunnen worden gepleegd, te rekenen vanaf het akkoord van de Commissie, en de motivering van de duur van deze periode;
	7° in voorkomend geval, de redenen die de hoogdringendheid bedoeld in paragraaf 6 rechtvaardigen;

	8° de naam van de agent(en) belast met de opvolging van het verloop van het strafbaar feit;
	9° de datum van de vraag;
	10° de handtekening van het diensthoofd.
	§4. De strafbare feiten moeten in gelijke verhouding staan tot het door de opdracht nagestreefde doel en mogen in geen geval afbreuk doen aan de fysieke integriteit van personen.
	§5. De agent belast met de opvolging van het verloop van het strafbaar feit brengt zo spoedig mogelijk na het plegen van het strafbaar feit schriftelijk verslag uit aan het diensthoofd.
	De betrokken inlichtingen- en veiligheidsdienst informeert zo spoedig mogelijk schriftelijk de Commissie.
	In afwijking van het tweede lid, indien de maatregel is toegestaan voor een periode langer dan twee maanden, brengt de betrokken inlichtingen- en veiligheidsdienst om de twee weken schriftelijk verslag uit aan de Commissie over het verloop van de maatregel.
	Op gemotiveerd verzoek van de Commissie wordt het verslag op een kortere termijn overgemaakt, voor zover de agent die het strafbaar feit pleegde in veiligheid is.
	§6. In geval van hoogdringendheid vraagt het diensthoofd vooraf het mondeling akkoord van de voorzitter van de Commissie of, indien hij niet bereikbaar is, van een ander lid. Diegene die het akkoord gegeven heeft, brengt de andere leden hiervan onmiddellijk op de hoogte. Het diensthoofd bevestigt zijn vraag schriftelijk binnen de vierentwintig uur na mededeling van het akkoord. Deze schriftelijke bevestiging bevat de vermeldingen bedoeld in paragraaf 3, lid 4. De voorzitter of het gecontacteerde lid bevestigt eveneens zo spoedig mogelijk schriftelijk zijn akkoord. Dit akkoord geldt voor vijf dagen.
	§7. Indien door onvoorziene omstandigheden feiten die als strafbaar feit of strafbare feiten

	kunnen worden gekwalificeerd gepleegd werden en waarvoor de procedure bedoeld in de paragrafen 3 of 6 niet gevolgd kon worden, brengt het diensthoofd dit zo spoedig mogelijk en ten laatste binnen de 24 uur vanaf zijn kennisname van het plegen van de feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd schriftelijk ter kennis van de Commissie. De agent die deze feiten heeft gepleegd blijft vrij van straf indien de Commissie oordeelt dat zij niet voorzienbaar en strikt noodzakelijk waren ter verzekering van de eigen veiligheid of die van derden.
	§8. Indien de Commissie nalaat haar beslissing te nemen overeenkomstig de paragrafen 3, 6 of 7, kan het betrokken diensthoofd het Vast Comité I vatten, dat zo spoedig mogelijk al dan niet de toestemming zal geven om het strafbaar feit of de strafbare feiten te plegen.
	In geval van een negatieve beslissing van de Commissie overeenkomstig de paragrafen 3, 6 of 7, kan het betrokken diensthoofd het Vast Comité I vatten. Het Vast Comité I zal zo spoedig mogelijk al dan niet de toestemming geven om het strafbaar feit of de strafbare feiten te plegen. Het Vast Comité I deelt zijn beslissing mee aan het diensthoofd en aan de Commissie.
	§9. De Commissie maakt alle documenten bedoeld in de paragrafen 3 tot 7 onverwijld over aan het Vast Comité I.
	§10. Het diensthoofd beëindigt de maatregel zo snel mogelijk wanneer de absolute noodzaak om een strafbaar feit te plegen weggevallen is, wanneer de maatregel niet langer nuttig is voor het doel waarvoor hij werd aangevraagd of wanneer een onwettigheid is vastgesteld. Hij brengt zijn beslissing zo snel mogelijk ter kennis van de Commissie en het Vast Comité I.
	Indien de Commissie of het Vast Comité I een onwettigheid vaststelt, brengt zij of hij het betrokken diensthoofd hier schriftelijk van op de hoogte. Deze laatste beëindigt zo snel mogelijk de geplande of lopende maatregel en bevestigt vervolgens schriftelijk aan de Commissie en aan het Vast Comité I dat de maatregel beëindigd is.

	§11. De leden van de Commissie kunnen op elk ogenblik een controle uitoefenen op de wettigheid van de maatregelen.
	Zij kunnen daartoe toegang hebben tot de gegevens met betrekking tot de maatregel, zich alle nuttige stukken toe-eigenen en de leden van de dienst horen.
	Art. 13/1/1.
	§1. Het is de menselijke bronnen verboden strafbare feiten te plegen.
	§2. In afwijking van paragraaf 1, blijven vrij van straf, de meerderjarige menselijke bronnen die, in het belang van de uitoefening van de opdrachten van de betrokken inlichtingen- en veiligheidsdienst, zoals bedoeld in de artikelen 7, 1° en 3°/1 en 11, §1, 1° tot 3° en 5°, strafbare feiten plegen die strikt noodzakelijk zijn ter verzekering van hun informatiepositie of ter verzekering van hun eigen veiligheid of die van derden.
	De strafbare feiten kunnen slechts worden gepleegd na voorafgaand schriftelijk akkoord van de Commissie. De Commissie geeft haar schriftelijk akkoord binnen de vier dagen na ontvangst van de schriftelijke en gemotiveerde vraag van het diensthoofd.
	Het akkoord geldt voor een maximumtermijn van twee maanden, onverminderd de mogelijkheid om de maatregel te verlengen volgens de procedure bedoeld in het tweede lid.
	Een risicoanalyse betreffende de betrouwbaarheid van de bron en de risico's waar zij zich aan blootstelt in het kader van het plegen van het strafbaar feit of de strafbare feiten moet worden uitgevoerd voorafgaand aan de vraag van het diensthoofd.
	De vraag van het diensthoofd vermeldt, op straffe van onwettigheid:
	1° de identificatiecode van de menselijke bron;
	2° de feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd;

	3° de context van de vraag en de finaliteit;
	4° de synthese van de risicoanalyse bedoeld in lid 4;
	5° de strikte noodzakelijkheid;
	6° de proportionaliteit bedoeld in paragraaf 3 ;
	7° de strikte voorwaarden opgelegd aan de menselijke bron;
	8° de periode tijdens dewelke strafbare feiten begaan kunnen worden en de motivering van de duur van deze periode;
	9° in voorkomend geval, de redenen die de hoogdringendheid bedoeld in paragraaf 6 rechtvaardigen;
	10° de naam van de agent(en) belast met de opvolging van het verloop van het strafbaar feit;
	11° de datum van de vraag;
	12° de handtekening van het diensthoofd.
	§3. De strafbare feiten moeten in gelijke verhouding staan tot het door de opdracht nagestreefde doel en mogen in geen geval afbreuk doen aan de fysieke integriteit van personen.
	§4. Vooraleer het toegelaten strafbaar feit kan worden gepleegd, ondertekent de menselijke bron een memorandum dat onder meer de modaliteiten voor de tenuitvoerlegging en de verslaggeving bevat. Dit memorandum wordt bewaard in het individueel dossier van de menselijke bron.
	Het memorandum wordt gedateerd en omvat onder meer de volgende vermeldingen:
	1° de identificatiecode van de menselijke bron;
	2° de wijze waarop het strafbaar feit ten uitvoer zal worden gelegd;

	3° de instructies en de strikte voorwaarden in het kader waarvan het strafbaar feit gepleegd mag worden;
	4° de rechten en plichten van de bron in het kader van het plegen van het toegelaten strafbaar feit;
	Een afschrift van het memorandum wordt overgemaakt aan de Commissie.
	§5. Zodra het strafbaar feit gepleegd is en de menselijke bron in veiligheid is, brengt deze verslag uit aan de agent belast met de opvolging van het verloop van het strafbaar feit. Deze laatste informeert schriftelijk het diensthoofd dat, op zijn beurt, zo spoedig mogelijk de Commissie schriftelijk informeert.
	Indien de maatregel werd toegestaan voor een periode langer dan twee weken, brengt de betrokken inlichtingen- en veiligheidsdienst om de twee weken schriftelijk verslag uit aan de Commissie over het verloop van de maatregel.
	Op gemotiveerd verzoek van de Commissie wordt het verslag op een kortere termijn overgemaakt, voor zover de agent en de bron in veiligheid zijn.
	§6. In geval van hoogdringendheid, wanneer uitzonderlijke omstandigheden en een ernstige potentiële dreiging dit rechtvaardigen, vraagt het diensthoofd het voorafgaand mondeling akkoord van de voorzitter van de Commissie of, indien hij niet bereikbaar, is van een ander lid. Diegene die het akkoord gegeven heeft, brengt de andere leden hier onmiddellijk van op de hoogte. Het diensthoofd bevestigt zijn vraag schriftelijk binnen de vierentwintig uur na mededeling van het akkoord. Deze schriftelijke bevestiging bevat de vermeldingen bedoeld in paragraaf 2, lid 5. De voorzitter of het gecontacteerde lid bevestigt eveneens zo snel mogelijk schriftelijk zijn akkoord. Dit akkoord geldt voor vijf dagen. De voorafgaandelijke voorwaarden bepaald in de paragrafen 2 tot 4 zijn van toepassing op deze paragraaf.
	§7. Indien de Commissie nalaat haar beslissing uit te brengen overeenkomstig de paragrafen 2 of 6, kan het betrokken diensthoofd het Vast Comité I vatten, dat zo spoedig mogelijk al dan niet de

	toestemming zal geven om het strafbaar feit of de strafbare feiten te plegen.
	In geval van een negatieve beslissing van de Commissie overeenkomstig de paragrafen 2 of 6, kan het betrokken diensthoofd het Vast Comité I vatten. Het Vast Comité I zal zo spoedig mogelijk al dan niet de toestemming geven om het strafbaar feit of de strafbare feiten te plegen.
	Het Vast Comité I deelt zijn beslissing mee aan het diensthoofd en aan de Commissie.
	§8. De Commissie maakt alle documenten bedoeld in de paragrafen 2 tot 5 onverwijld over aan het Vast Comité I.
	§9. Het diensthoofd beëindigt de maatregel zo snel mogelijk, wanneer de absolute noodzaak om een strafbaar feit te plegen weggevallen is, wanneer de maatregel niet langer nuttig is voor het doel waarvoor hij werd aangevraagd of wanneer een onwettigheid is vastgesteld. Hij brengt zijn beslissing zo snel mogelijk ter kennis van de Commissie.
	Indien de Commissie of het Vast Comité I een onwettigheid vaststelt, brengt zij of hij het betrokken diensthoofd hiervan op de hoogte, dat de geplande of lopende maatregel zo snel mogelijk beëindigt. Deze laatste bevestigt vervolgens schriftelijk aan de Commissie en aan het Vast Comité I dat de maatregel beëindigd is.
	§10. De leden van de Commissie kunnen op elk ogenblik een controle uitoefenen op de wettigheid van de maatregelen.
	Zij kunnen daartoe toegang hebben tot de papieren versie van de documenten met betrekking tot het plegen van een strafbaar feit of strafbare feiten door de bron en de agent horen die belast is met de opvolging van het verloop van het strafbaar feit, in het bijzijn van zijn hiërarchische meerdere, en ieder ander die verantwoordelijk is voor de behandeling van voornoemde bron.
	Art. 13/1/2.

	§1. In de toepassing van de artikelen 13/1 en 13/1/1, treedt de Commissie op volgens de modaliteiten bepaald in artikel 43/1.
	§2. Blijven vrij van straf, de leden van de Commissie die een akkoord verlenen tot het plegen van strafbare feiten zoals bedoeld in de artikelen 13/1 en 13/1/1.
	§3. Blijven vrij van straf, de raadsleden en de medewerkers van het Vast Comité I wanneer zij hun toezicht uitoefenen binnen de toepassing van deze onderafdeling.
	§4. Blijven vrij van straf, de agenten van de inlichtingen- en veiligheidsdiensten die de agenten bedoeld in artikel 13/1 en de menselijke bronnen bedoeld in artikel 13/1/1, begeleiden of controleren.
	<u>Onderafdeling 2.- Valse naam, valse hoedanigheid, fictieve identiteit en fictieve hoedanigheid</u>
Art. 13/2.	**Art. 13/2.**
Een agent kan, om veiligheidsredenen verbonden aan de bescherming van zijn persoon of van derden, gebruik maken van een naam die hem niet toebehoort alsook van een fictieve identiteit en hoedanigheid, volgens de door de Koning te bepalen nadere regels.	Een agent kan, om veiligheidsredenen verbonden aan de bescherming van zijn persoon of van derden, gebruik maken van een **valse naam, een valse hoedanigheid, een fictieve identiteit of een fictieve hoedanigheid** volgens de door de Koning **bepaalde** nadere regels.
De in het eerste lid bedoelde maatregel mag niet autonoom aangewend worden voor het verzamelen van gegevens.	De in het eerste lid bedoelde maatregel mag niet autonoom aangewend worden voor het verzamelen van gegevens.
Elk actief gebruik van een fictieve identiteit dient tijdelijk en doelgericht te zijn en wordt vermeld in een lijst die maandelijks overgemaakt wordt aan het Vast Comité I.	Elk actief gebruik van een fictieve identiteit dient doelgericht te zijn en wordt vermeld in een lijst die maandelijks overgemaakt wordt aan het Vast Comité I.
De inlichtingen- en veiligheidsdiensten kunnen, in het kader van de aanmaak en het gebruik van een valse naam of van een fictieve identiteit en hoedanigheid, valse documenten vervaardigen, laten vervaardigen en gebruiken.	De inlichtingen- en veiligheidsdiensten kunnen, in het kader van de aanmaak en het gebruik van een valse naam, **van een valse hoedanigheid**, van een fictieve identiteit **of** hoedanigheid, valse documenten vervaardigen, laten vervaardigen en gebruiken.
Elke aanmaak van officiële documenten ten bewijze van een fictieve identiteit of	Elke aanmaak van officiële documenten ten bewijze van een fictieve identiteit of hoedanigheid

hoedanigheid wordt gemachtigd door het diensthoofd en wordt ter kennis gebracht van het Vast Comité I.	wordt gemachtigd door het diensthoofd en wordt ter kennis gebracht van het Vast Comité I.
In het kader van de uitvoering van de in dit artikel bedoelde maatregelen kunnen de inlichtingen- en veiligheidsdiensten de medewerking vorderen van de ambtenaren en agenten van de openbare diensten.	In het kader van de uitvoering van de in dit artikel bedoelde maatregelen kunnen de inlichtingen- en veiligheidsdiensten de medewerking vorderen van de ambtenaren en agenten van de openbare diensten.
	Onderafdeling 3.- De oprichting en inzet van rechtspersonen
Art. 13/3.	**Art. 13/3.**
§ 1. De inlichtingen- en veiligheidsdiensten kunnen rechtspersonen 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.	§ 1. De inlichtingen- en veiligheidsdiensten kunnen rechtspersonen 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.
§ 2. De inlichtingen- en veiligheidsdiensten kunnen rechtspersonen inzetten ter ondersteuning van hun opdrachten.	§ 2. De inlichtingen- en veiligheidsdiensten kunnen rechtspersonen inzetten ter ondersteuning van hun opdrachten.
Onverminderd het eerste lid, worden de nadere regels voor het inzetten van een rechtspersoon voor het verzamelen van gegevens bepaald in artikel 18/13.	Onverminderd het eerste lid, worden de nadere regels voor het inzetten van een rechtspersoon voor het verzamelen van gegevens bepaald in artikel 18/13.
§ 3. De inlichtingen- en veiligheidsdiensten kunnen, in het kader van de toepassing van paragrafen 1 en 2, valse documenten vervaardigen, laten vervaardigen en gebruiken.	§ 3. De inlichtingen- en veiligheidsdiensten kunnen, in het kader van de toepassing van paragrafen 1 en 2, valse documenten vervaardigen, laten vervaardigen en gebruiken.
§ 4. Elke oprichting van een rechtspersoon wordt gemachtigd door het diensthoofd en wordt ter kennis gebracht van het Vast Comité I.	§ 4. Elke oprichting van een rechtspersoon wordt gemachtigd door het diensthoofd en wordt ter kennis gebracht van het Vast Comité I.
Elke inzet van een rechtspersoon buiten het geval voorzien in artikel 18/13, wordt vermeld in een lijst die maandelijks overgemaakt wordt aan het Vast Comité I.	Elke inzet van een rechtspersoon buiten het geval voorzien in artikel 18/13, wordt vermeld in een lijst die maandelijks overgemaakt wordt aan het Vast Comité I.
§ 5. In het kader van de uitvoering van dit artikel kunnen de inlichtingen- en veiligheidsdiensten de medewerking vorderen	§ 5. In het kader van de uitvoering van dit artikel kunnen de inlichtingen- en veiligheidsdiensten de medewerking vorderen van de ambtenaren en agenten van de openbare diensten.

van de ambtenaren en agenten van de openbare diensten.	
	Onderafdeling 4.- De medewerking van derden
Art. 13/4.	**Art. 13/4.**
De inlichtingen- en veiligheidsdiensten kunnen de medewerking van derden verzoeken.	De inlichtingen- en veiligheidsdiensten kunnen de medewerking van derden verzoeken.
De diensten waken over de veiligheid van de gegevens die betrekking hebben op de derden die een medewerking aan hen verlenen of hebben verleend.	De diensten waken over de veiligheid van de gegevens die betrekking hebben op de derden die een medewerking aan hen verlenen of hebben verleend.
Het tweede, derde en vijfde lid van artikel 13/1 zijn van toepassing op de derden die aan de uitvoering van een methode noodzakelijke en rechtstreekse hulp en bijstand hebben verleend.	**De paragrafen 2 tot 6 en 8 tot 9 van artikel 13/1 en paragraaf 11 van artikel 13/1/1 zijn van toepassing op de derden die noodzakelijke en rechtstreekse hulp en bijstand verlenen voor de toepassing van deze wet.**
	De verleende hulp en bijstand geschiedt te allen tijde onder het toezicht van de betrokken inlichtingen- en veiligheidsdienst, die de leiding behoudt over de operatie.
Art. 16/3.	**Art. 16/3.**
§ 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, mits afdoende motivering, beslissen om toegang te hebben tot de passagiersgegevens bedoeld in artikel 27 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens.	§ 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, mits afdoende motivering, beslissen om toegang te hebben tot de passagiersgegevens bedoeld in artikel 27 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens.
§ 2. De in § 1 bedoelde beslissing, wordt door een diensthoofd genomen en schriftelijk overgemaakt aan de Passagiersinformatie-eenheid bedoeld in hoofdstuk 7 van voormelde wet. De beslissing wordt met de motivering van deze beslissing aan het Vast Comité I betekend.	§ 2. De in § 1 bedoelde beslissing, wordt door **het diensthoofd of zijn gedelegeerde** genomen en schriftelijk overgemaakt aan de Passagiersinformatie-eenheid bedoeld in hoofdstuk 7 van voormelde wet. De beslissing wordt met de motivering van deze beslissing aan het Vast Comité I betekend.
	In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde mondeling beslissen om toegang te hebben tot deze gegevens. Deze mondelinge beslissing wordt de eerste werkdag volgend op de datum van de

	beslissing bevestigd door een schriftelijke beslissing, volgens de nadere regels bepaald in het eerste lid.
Het Vast Comité I verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke voorwaarden voldoen.	Het Vast Comité I verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke **bepalingen** voldoen.
De beslissing kan betrekking hebben op een geheel van gegevens die betrekking hebben op een specifiek inlichtingenonderzoek. In dit geval wordt de lijst van de raadplegingen van de passagiersgegevens een keer per maand aan het Vast Comité I doorgegeven.	De beslissing kan betrekking hebben op een geheel van gegevens die betrekking hebben op een specifiek inlichtingenonderzoek. In dit geval wordt de lijst van de raadplegingen van de passagiersgegevens een keer per maand aan het Vast Comité I doorgegeven.
Art. 16/4.	**Art. 16/4.**
§ 1. Overeenkomstig de nadere regels bepaald door de Koning, na advies van de bevoegde toezichthoudende autoriteit voor de verwerking van persoonsgegevens, is een rechtstreekse toegang toegestaan voor de inlichtingen- en veiligheidsdiensten tot de informatie en persoonsgegevens die verzameld worden door middel van camera's waarvan het gebruik door de politiediensten is toegestaan overeenkomstig hoofdstuk IV, afdeling 1, en hoofdstuk IV/1, afdeling 2, van de wet op het politieambt en die in het bijzonder worden verwerkt in de gegevensbanken bedoeld in artikel 44/2 van de genoemde wet.	§ 1. Overeenkomstig de nadere regels bepaald door de Koning, na advies van de bevoegde toezichthoudende autoriteit voor de verwerking van persoonsgegevens, is een rechtstreekse toegang toegestaan voor de inlichtingen- en veiligheidsdiensten tot de informatie en persoonsgegevens die verzameld worden door middel van camera's waarvan het gebruik door de politiediensten is toegestaan overeenkomstig hoofdstuk IV, afdeling 1, en hoofdstuk IV/1, afdeling 2, van de wet op het politieambt en die in het bijzonder worden verwerkt in de gegevensbanken bedoeld in artikel 44/2 van de genoemde wet.
In afwijking van artikelen 25/5, § 2, en 46/2 van de wet op het politieambt, oefenen de politiediensten geen controle uit op het bekijken van beelden in real time door de inlichtingen- en veiligheidsdiensten.	In afwijking van artikelen 25/5, § 2, en 46/2 van de wet op het politieambt, oefenen de politiediensten geen controle uit op het bekijken van beelden in real time door de inlichtingen- en veiligheidsdiensten.
De informatie en persoonsgegevens bedoeld in het eerste lid kunnen na anonimisering worden gebruikt voor didactische en pedagogische doeleinden in het kader van de opleiding van de leden van de inlichtingen- en veiligheidsdiensten.	De informatie en persoonsgegevens bedoeld in het eerste lid kunnen na anonimisering worden gebruikt voor didactische en pedagogische doeleinden in het kader van de opleiding van de leden van de inlichtingen- en veiligheidsdiensten.

§ 2. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, op gerichte wijze en na hun registratie toegang nemen tot de informatie en persoonsgegevens van de gegevensbanken bedoeld in artikels 25/6, 44/2, § 3, tweede lid, 1° en 2°, en 46/12 van de wet op het politieambt, indien dit gemotiveerd wordt op operationeel vlak, noodzakelijk is voor de uitoefening van een precieze opdracht en beslist wordt door een inlichtingenofficier.	§ 2. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, op gerichte wijze en na hun registratie toegang nemen tot de informatie en persoonsgegevens van de gegevensbanken bedoeld in **de artikelen** 25/6, 44/2, § 3, tweede lid, 1° en 2°, en 46/12 van de wet op het politieambt, indien dit gemotiveerd wordt op operationeel vlak, noodzakelijk is voor de uitoefening van een precieze opdracht en beslist wordt door een **methodenofficier**.
Na de eerste maand van bewaring, wordt de toegang tot de gegevens bedoeld in deze paragraaf toegestaan door het diensthoofd of zijn gedelegeerde.	Na de eerste maand van bewaring, wordt de toegang tot de gegevens bedoeld in deze paragraaf toegestaan door het diensthoofd of zijn gedelegeerde.
	In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde mondeling beslissen om toegang te hebben tot deze gegevens. Deze mondelinge beslissing wordt de eerste werkdag volgend op de datum van de beslissing bevestigd door een schriftelijke beslissing volgens de nadere regels bepaald in het vierde lid.
De beslissing van het diensthoofd of zijn gedelegeerde wordt met de motivering van deze beslissing zo spoedig mogelijk aan het Vast Comité I betekend. De beslissing kan betrekking hebben op een geheel van gegevens die betrekking hebben op een specifiek inlichtingenonderzoek. In dit geval wordt een lijst van de gerichte toegangen een maal per maand aan het Vast Comité I doorgegeven. Het Vast Comité I verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke voorwaarden voldoen.	De beslissing van het diensthoofd of zijn gedelegeerde wordt met de motivering van deze beslissing zo spoedig mogelijk aan het Vast Comité I betekend. De beslissing kan betrekking hebben op een geheel van gegevens die betrekking hebben op een specifiek inlichtingenonderzoek. In dit geval wordt een lijst van de gerichte toegangen een maal per maand aan het Vast Comité I doorgegeven. Het Vast Comité I verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke **bepalingen** voldoen.
De toegang tot deze informatie en persoonsgegevens is beveiligd, alle toegangen worden dagelijks bijgewerkt en de concrete redenen van de bevragingen worden geregistreerd.	De toegang tot deze informatie en persoonsgegevens is beveiligd, alle toegangen worden dagelijks bijgewerkt en de concrete redenen van de bevragingen worden geregistreerd.
§ 3. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de informatie en persoonsgegevens van de gegevensbanken	§ 3. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de informatie en persoonsgegevens van de gegevensbanken bedoeld in artikel 44/2, §

bedoeld in artikel 44/2, § 3, tweede lid, 1° en 2°, van de wet op het politieambt in correlatie brengen met :	3, tweede lid, 1° en 2°, van de wet op het politieambt in correlatie brengen met :
1° de gegevensbanken beheerd door de inlichtingen- en veiligheidsdiensten of die voor hen rechtstreeks beschikbaar of toegankelijk zijn in het kader van hun opdrachten, of lijsten van personen uitgewerkt door de inlichtingen- en veiligheidsdiensten in het kader van hun opdrachten;	1° de gegevensbanken beheerd door de inlichtingen- en veiligheidsdiensten of die voor hen rechtstreeks beschikbaar of toegankelijk zijn in het kader van hun opdrachten, of lijsten van personen uitgewerkt door de inlichtingen- en veiligheidsdiensten in het kader van hun opdrachten;
2° vooraf bepaalde beoordelingscriteria. De gegevensbanken of lijsten of de vooraf bepaalde beoordelingscriteria bedoeld in deze paragraaf worden voorbereid met als doel deze correlatie tot stand te brengen na registratie van de gegevens.	2° vooraf bepaalde beoordelingscriteria. De gegevensbanken of lijsten of de vooraf bepaalde beoordelingscriteria bedoeld in deze paragraaf worden voorbereid met als doel deze correlatie tot stand te brengen na registratie van de gegevens.
De inhoud van de gegevensbanken of van de lijsten bedoeld in het eerste lid, 1°, die gebruikt worden voor een correlatie, is onderworpen aan de toelating van een inlichtingenofficier. De beslissing om de gegevensbanken of de lijsten in correlatie te brengen, kan slaan op een geheel van gegevens die betrekking hebben op een of meerdere specifieke inlichtingenonderzoeken.	De inhoud van de gegevensbanken of van de lijsten bedoeld in het eerste lid, 1°, die gebruikt worden voor een correlatie, is onderworpen aan de toelating van een **methodenofficier**. De beslissing om de gegevensbanken of de lijsten in correlatie te brengen, kan slaan op een geheel van gegevens die betrekking hebben op een of meerdere specifieke inlichtingenonderzoeken.
Elke lijst aan de hand waarvan de correlatie bedoeld in het eerste lid, 1°, wordt uitgevoerd, wordt zo spoedig mogelijk doorgegeven aan het Vast Comité I. Het Vast Comité I verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke voorwaarden voldoen.	Elke lijst aan de hand waarvan de correlatie bedoeld in het eerste lid, 1°, wordt uitgevoerd, wordt zo spoedig mogelijk doorgegeven aan het Vast Comité I. Het Vast Comité I verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke **bepalingen** voldoen.
De beoordelingscriteria bedoeld in het eerste lid, 2°, worden voorafgaandelijk aan het Vast Comité I voorgelegd. Correlaties die deze beoordelingscriteria verder verfijnen, dienen niet meer opnieuw voorgelegd te worden. Deze beoordelingscriteria mogen niet gericht zijn op de identificatie van een individu en moeten doelgericht, evenredig en specifiek zijn.	De beoordelingscriteria bedoeld in het eerste lid, 2°, worden voorafgaandelijk aan het Vast Comité I voorgelegd. Correlaties die deze beoordelingscriteria verder verfijnen, dienen niet meer opnieuw voorgelegd te worden. Deze beoordelingscriteria mogen niet gericht zijn op de identificatie van een individu en moeten doelgericht, evenredig en specifiek zijn.
§ 4. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, toegang krijgen tot het	§ 4. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, toegang krijgen tot het register

register bedoeld in artikel 25/8, tweede lid, van de wet op het politieambt.	bedoeld in artikel 25/8, tweede lid, van de wet op het politieambt.
§ 5. In geval de rechtstreekse toegang bedoeld in dit artikel mogelijk is, kan een inlichtingen- en veiligheidsdienst niet eenzelfde rechtstreekse toegang verzoeken op basis van artikel 14, tweede lid.	§ 5. In geval de rechtstreekse toegang bedoeld in dit artikel mogelijk is, kan een inlichtingen- en veiligheidsdienst niet eenzelfde rechtstreekse toegang verzoeken op basis van artikel 14, tweede lid.
De bevoegde magistraat die oordeelt dat een rechtstreekse toegang tot de informatie en persoonsgegevens het goede verloop van een opsporingsonderzoek of gerechtelijk onderzoek kan schaden, kan besluiten om die toegang tijdelijk onmogelijk te maken. Indien een inlichtingen- en veiligheidsdienst ten aanzien van deze informatie en persoonsgegevens gebruik maakt van de rechtstreekse toegang, wordt haar meegedeeld dat deze onvolledig zijn.	De bevoegde magistraat die oordeelt dat een rechtstreekse toegang tot de informatie en persoonsgegevens het goede verloop van een **opsporings- of gerechtelijk onderzoek** kan schaden, kan besluiten om die toegang tijdelijk onmogelijk te maken. Indien een inlichtingen- en veiligheidsdienst ten aanzien van deze informatie en persoonsgegevens gebruik maakt van de rechtstreekse toegang, wordt haar meegedeeld dat deze onvolledig zijn.
§ 6. De inlichtingenofficier die de beslissingen voorzien in dit artikel neemt, kan niet tegelijk de beheerder zijn van het dossier waarop die beslissing betrekking heeft.	§ 6. De **methodenofficier** die de beslissingen voorzien in dit artikel neemt, kan niet tegelijk de beheerder zijn van het dossier waarop die beslissing betrekking heeft.
	Art. 16/5.
	De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, in de virtuele wereld infiltreren, al dan niet onder dekmantel van een valse naam of valse hoedanigheid.
	Art. 16/6.
	§ 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van:
	1° de personen en instellingen bedoeld in artikel 5, paragraaf 1, 3° tot 22° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;
	2° de personen en instellingen die, binnen het Belgisch grondgebied, diensten beschikbaar stellen of aanbieden met betrekking tot virtuele waarden die toelaten dat gereglementeerde

	betaalmiddelen in virtuele waarden worden uitgewisseld;
	3° het Centraal Aanspreekpunt gehouden door de Nationale Bank van België overeenkomstig de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van bankrekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest;
	om over te gaan tot:
	a) het identificeren van de producten en diensten, waarvan de geviseerde persoon titularis, gevolmachtigde of de uiteindelijke gerechtigde is;
	b) het identificeren van de titularissen, de gevolmachtigden, of de uiteindelijke gerechtigden van de producten en diensten.
	De vordering bedoeld in het eerste lid, 1° en 2° gebeurt schriftelijk door het diensthoofd of zijn gedelegeerde. In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde deze gegevens mondeling vorderen. Deze mondelinge vordering wordt binnen de vierentwintig uur bevestigd door een schriftelijke vordering.
	De gevorderde medewerking bedoeld in het eerste lid, 3° gebeurt na schriftelijke beslissing van het diensthoofd of zijn gedelegeerde, en overeenkomstig de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van bankrekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest. In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde de methode mondeling toestaan. Deze mondelinge beslissing wordt binnen de vierentwintig uur bevestigd door een schriftelijke beslissing.
	§ 2. De gevorderde persoon of instelling is ertoe gehouden de gevraagde informatie onverwijld te verstrekken na ontvangst van de schriftelijke vordering van het diensthoofd of zijn gedelegeerde.

	De gevorderde persoon of instelling die de in dit artikel bedoelde medewerking weigert te verlenen, wordt gestraft met geldboete van zesentwintig euro tot twintigduizend euro.
	§ 3. Beide inlichtingen- en veiligheidsdiensten houden een register bij van alle gevorderde identificaties. De betrokken inlichtingen- en veiligheidsdienst maakt maandelijks een lijst van de gevorderde identificaties over aan het Vast Comité I.
	Het Vast Comité I verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke bepalingen voldoen.
Art. 18.	**Art. 18.**
De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, een beroep doen op menselijke bronnen voor het verzamelen van gegevens omtrent gebeurtenissen, voorwerpen, groeperingen en natuurlijke personen of rechtspersonen die een belang vertonen voor de uitoefening van hun opdrachten, conform de richtlijnen van de Nationale Veiligheidsraad.	**§1.** De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, een beroep doen op **personen waaronder** menselijke bronnen voor het verzamelen van gegevens omtrent gebeurtenissen, voorwerpen, groeperingen en natuurlijke personen of rechtspersonen die een belang vertonen voor de uitoefening van hun opdrachten, conform de richtlijnen van de Nationale Veiligheidsraad.
	§2. In het belang van de uitvoering van hun opdrachten bedoeld in de artikelen 7, 1° en 3°/1 en 11, §1, 1° tot 3° en 5° , kunnen de inlichtingen- en veiligheidsdiensten de methoden voor het verzamelen van gegevens aanwenden ten opzichte van een menselijke bron:
	1° indien er twijfel bestaat over zijn betrouwbaarheid, discretie of loyauteit tegenover de betrokken inlichtingen- en veiligheidsdienst waardoor een nadeel ontstaat voor de uitoefening van de opdrachten van die dienst, of
	2° ter verzekering van zijn bescherming.
Art. 18/1	**Art. 18/1**
Deze onderafdeling is van toepassing :	Deze onderafdeling is van toepassing :

1° op de Veiligheid van de Staat voor de uitoefening, op of vanaf het grondgebied van het Rijk, van de opdrachten bedoeld in de artikelen 7, 1° en 3° /1, […], onverminderd artikel 18/9, § 1, 1°;	1° op de Veiligheid van de Staat voor de uitoefening, op of vanaf het grondgebied van het Rijk, van de opdrachten bedoeld in de artikelen 7, 1° en 3° /1, […], onverminderd artikel 18/9, § 1, 1°;
2° op de Algemene Dienst Inlichting en Veiligheid, onverminderd artikel 18/9, § 1, 2°, voor de uitoefening van de opdrachten bedoeld in de artikelen 11, § 1, 1° tot 3° en 5°, en § 2, met uitzondering van de interceptie van communicatie uitgezonden of ontvangen in het buitenland alsook het binnendringen in een informaticasysteem dat zich in het buitenland bevindt en het maken van vaste of bewegende beelden uitgevoerd in het buitenland, bedoeld in de artikelen 44 tot 44/5.	2° op de Algemene Dienst Inlichting en Veiligheid, onverminderd artikel 18/9, § 1, 2°, voor de uitoefening van de opdrachten bedoeld in de artikelen 11, § 1, 1° tot 3° en 5°, en § 2, met uitzondering van de interceptie van communicatie uitgezonden of ontvangen in het buitenland alsook het binnendringen in een informaticasysteem dat zich in het buitenland bevindt en het maken van vaste of bewegende beelden uitgevoerd in het buitenland, bedoeld in de artikelen 44 tot 44/5**;**
	3° onverminderd 1° en 2°, op de inlichtingen- en veiligheidsdiensten, in het kader van artikel 18, paragraaf 2.
Art. 18/2	**Art. 18/2**
§ 1. De specifieke methoden voor het verzamelen van gegevens worden opgesomd in de artikelen 18/4 tot 18/8.	§ 1. De specifieke methoden voor het verzamelen van gegevens worden opgesomd in de artikelen 18/4 tot 18/8.
§ 2. De uitzonderlijke methoden voor het verzamelen van gegevens worden opgesomd in de artikelen 18/11 tot 18/17.	§ 2. De uitzonderlijke methoden voor het verzamelen van gegevens worden opgesomd in de artikelen 18/11 tot 18/17.
§ 3. Als een in § § 1 en 2 bedoelde methode aangewend wordt ten opzichte van een advocaat, een arts of een journalist, of van hun lokalen of communicatiemiddelen die zij voor beroepsdoeleinden gebruiken, of van hun woonplaats of verblijfplaats, mag deze methode niet uitgevoerd worden zonder dat, naargelang het geval, de voorzitter van de Orde van de Vlaamse balies, van de Ordre des barreaux francophones et germanophone, van de Nationale Raad van de Orde van Geneesheren of van de Vereniging van Beroepsjournalisten of in geval van ziekte of verhindering van de voorzitter diens plaatsvervanger hiervan vooraf op de hoogte is gebracht door de voorzitter van de commissie bedoeld in artikel 3, 6°. De voorzitter van de	§ 3. Als een in **de paragrafen** 1 en 2 bedoelde methode aangewend wordt ten opzichte van een advocaat, een arts of een journalist, of van hun lokalen of communicatiemiddelen die zij voor beroepsdoeleinden gebruiken, of van hun woonplaats of verblijfplaats, mag deze methode niet uitgevoerd worden zonder dat, naargelang het geval, de voorzitter van de Orde van de Vlaamse balies, van de Ordre des barreaux francophones et germanophone, van de Nationale Raad van de Orde van Geneesheren of van de Vereniging van Beroepsjournalisten of in geval van ziekte of verhindering van de voorzitter diens plaatsvervanger hiervan vooraf op de hoogte is gebracht door de voorzitter van de **Commissie of, bij verhindering, door een ander Commissielid**. De voorzitter van de commissie **of het**

commissie is verplicht om de nodige inlichtingen te verstrekken aan de voorzitter van de Orde of van de Vereniging van Beroepsjournalisten, waarvan de advocaat, de arts of de journalist deel uitmaakt of aan de plaatsvervanger van de voorzitter. De betrokken voorzitter en zijn plaatsvervanger zijn tot geheimhouding verplicht. De straffen bepaald in artikel 458 van het Strafwetboek zijn van toepassing voor inbreuken op deze verplichting tot geheimhouding.	**Commissielid dat de voorzitter vervangt,** is verplicht om de nodige inlichtingen te verstrekken aan de voorzitter van de Orde of van de Vereniging van Beroepsjournalisten, waarvan de advocaat, de arts of de journalist deel uitmaakt of aan de plaatsvervanger van de voorzitter. De betrokken voorzitter en zijn plaatsvervanger zijn tot geheimhouding verplicht. De straffen bepaald in artikel 458 van het Strafwetboek zijn van toepassing voor inbreuken op deze verplichting tot geheimhouding.
Als een in §§ 1 en 2 bedoelde methode aangewend wordt ten opzichte van een advocaat, een arts of een journalist, van hun lokalen of communicatiemiddelen die zij voor beroepsdoeleinden gebruiken, of van hun woonplaats of verblijfplaats, gaat de voorzitter van de commissie na of de via deze methode verkregen gegevens een rechtstreeks verband hebben met de potentiële dreiging, wanneer zij beschermd worden door het beroepsgeheim van een advocaat of arts of door het bronnengeheim van een journalist. Zo geen rechtstreeks verband is aangetoond, verbiedt de Commissie de inlichtingen- en veiligheidsdiensten deze gegevens te exploiteren.	Als een in **paragrafen** 1 en 2 bedoelde methode aangewend wordt ten opzichte van een advocaat, een arts of een journalist, van hun lokalen of communicatiemiddelen die zij voor beroepsdoeleinden gebruiken, of van hun woonplaats of verblijfplaats, gaat de voorzitter van de commissie **of, bij verhindering, een ander Commissielid,** na of de via deze methode verkregen gegevens een rechtstreeks verband hebben met de potentiële dreiging, wanneer zij beschermd worden door het beroepsgeheim van een advocaat of arts of door het bronnengeheim van een journalist. Zo geen rechtstreeks verband is aangetoond, verbiedt de Commissie de inlichtingen- en veiligheidsdiensten deze gegevens te exploiteren.
Als een in § 2 bedoelde uitzonderlijke methode aangewend wordt ten opzichte van een advocaat, een arts of een journalist, kan de voorzitter van de commissie of het door hem aangewezen lid van de commissie aanwezig zijn bij de aanwending van deze methode. De voorzitter houdt rekening met het risico dat zijn aanwezigheid kan hebben voor de uitoefening van de opdracht, zijn eigen veiligheid en de veiligheid van de agenten en van derden.	Als een in **paragraaf** 2 bedoelde uitzonderlijke methode aangewend wordt ten opzichte van een advocaat, een arts of een journalist, kan de voorzitter van de commissie of het door hem aangewezen lid van de commissie aanwezig zijn bij de aanwending van deze methode. De voorzitter houdt rekening met het risico dat zijn aanwezigheid kan hebben voor de uitoefening van de opdracht, zijn eigen veiligheid en de veiligheid van de agenten en van derden.
	§4. Indien een in de paragrafen 1 en 2 bedoelde methode wordt aangewend ten opzichte van een menselijke bron in toepassing van artikel 18, § 2, wordt van de op straffe van nietigheid voorgeschreven vermeldingen bepaald in de artikelen 18/3, § 2, 2° en 3° en 18/10, § 2, 2° en 3° afgeweken.
Art. 18/3	**Art. 18/3**

§ 1. Rekening houdend met een potentiële dreiging zoals bedoeld in artikel 18/1 kunnen de in artikel 18/2, § 1, bedoelde specifieke methoden voor het verzamelen van gegevens aangewend worden indien de gewone methoden voor het verzamelen van gegevens ontoereikend worden geacht om de informatie te verzamelen die nodig is om de inlichtingenopdracht te volbrengen. De specifieke methode moet worden gekozen in functie van de graad van ernst van de potentiële dreiging waarvoor ze wordt aangewend.	§ 1. Rekening houdend met een potentiële dreiging zoals bedoeld in artikel 18/1 **of in het kader van artikel 18, § 2,** kunnen de in artikel 18/2, § 1, bedoelde specifieke methoden voor het verzamelen van gegevens aangewend worden indien de gewone methoden voor het verzamelen van gegevens ontoereikend worden geacht om de informatie te verzamelen die nodig is om de inlichtingenopdracht te volbrengen. De specifieke methode moet worden gekozen in functie van de graad van ernst van de potentiële dreiging waarvoor ze wordt aangewend **of in functie van de graad van ernst van het potentieel nadeel voor de uitoefening van de opdrachten van de diensten of het potentiële gevaar voor de veiligheid van de menselijke bron in het kader van artikel 18, §2.**
De specifieke methode kan slechts worden aangewend na een schriftelijke en met redenen omklede beslissing van het diensthoofd en na kennisgeving van deze beslissing aan de commissie.	De specifieke methode kan slechts worden aangewend na een schriftelijke en met redenen omklede beslissing van het diensthoofd en na kennisgeving van deze beslissing aan de commissie.
§ 2. De beslissing van het diensthoofd vermeldt:	§ 2. De beslissing van het diensthoofd vermeldt:
1° de aard van de specifieke methode;	1° de aard van de specifieke methode;
2° naargelang het geval, de natuurlijke personen of rechtspersonen, feitelijke verenigingen of groeperingen, voorwerpen, plaatsen, gebeurtenissen of informatie die het voorwerp uitmaken van de specifieke methode;	2° naargelang het geval, de natuurlijke personen of rechtspersonen, feitelijke verenigingen of groeperingen, voorwerpen, plaatsen, gebeurtenissen of informatie die het voorwerp uitmaken van de specifieke methode;
3° de potentiële dreiging die de specifieke methode rechtvaardigt;	3° de potentiële dreiging die de specifieke methode rechtvaardigt;
4° de feitelijke omstandigheden die de specifieke methode rechtvaardigen, de motivering inzake subsidiariteit en proportionaliteit, inbegrepen het verband tussen de bepalingen onder 2° en 3°;	4° de feitelijke omstandigheden die de specifieke methode rechtvaardigen, de motivering inzake subsidiariteit en proportionaliteit, inbegrepen het verband tussen de bepalingen onder 2° en 3°;
5° de periode waarin de specifieke methode kan worden aangewend, te rekenen vanaf de kennisgeving van de beslissing aan de Commissie;	5° de periode waarin de specifieke methode kan worden aangewend, te rekenen vanaf de kennisgeving van de beslissing aan de Commissie;

6° de naam van de inlichtingenofficier(en) verantwoordelijk om de aanwending van de specifieke methode op te volgen;	6° de naam van de **methodenofficier**(en) verantwoordelijk om de aanwending van de specifieke methode op te volgen;
7° in voorkomend geval, het technisch middel dat gebruikt wordt bij de aanwending van de specifieke methode in toepassing van de artikelen 18/4 of 18/5;	7° in voorkomend geval, het technisch middel dat gebruikt wordt bij de aanwending van de specifieke methode in toepassing van de artikelen 18/4 of 18/5;
8° in voorkomend geval, de samenloop met een opsporings- of gerechtelijk onderzoek;	8° in voorkomend geval, de samenloop met een opsporings- of gerechtelijk onderzoek;
9° in voorkomend geval, de strafbare feiten die strikt noodzakelijk zijn voor het welslagen van de uitvoering van de methode of ter verzekering van de veiligheid van de agenten of derden;	9° in voorkomend geval, **de feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd** die strikt noodzakelijk zijn voor het welslagen van de uitvoering van de methode of ter verzekering van de veiligheid van de agenten of derden;
10° in voorkomend geval, de ernstige aanwijzingen waaruit blijkt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of de ontwikkeling van de potentiële dreiging;	10° in voorkomend geval, de ernstige aanwijzingen waaruit blijkt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of de ontwikkeling van de potentiële dreiging;
11° in voorkomend geval, de redenen die de hoogdringendheid rechtvaardigen;	11° in voorkomend geval, de redenen die de hoogdringendheid rechtvaardigen;
12° in geval toepassing wordt gemaakt van artikel 18/8, de motivering van de duur van de periode waarop de inzameling van gegevens betrekking heeft;	12° in geval toepassing wordt gemaakt van artikel 18/8, de motivering van de duur van de periode waarop de inzameling van gegevens betrekking heeft;
13° de datum van de beslissing;	13° de datum van de beslissing;
14° de handtekening van het diensthoofd.	14° de handtekening van het diensthoofd.
De vermeldingen bedoeld in de bepalingen onder 1° tot 4°, 7°, 9°, 10°, 11° en 14° zijn op straffe van onwettigheid voorgeschreven.	De vermeldingen bedoeld in de bepalingen onder 1° tot 4°, 7°, 9°, 10°, 11° en 14° zijn op straffe van onwettigheid voorgeschreven.
	In het kader van artikel 18, §2 en in afwijking van paragraaf 2, 2° en 3°, vermeldt de beslissing van het diensthoofd respectievelijk de identificatiecode van de menselijke bron en het potentieel nadeel voor de uitoefening van de opdrachten van de diensten of het potentiële gevaar voor de veiligheid van de menselijke bron.

§ 3. In geval van hoogdringendheid kan het diensthoofd de specifieke methode mondeling toestaan. Deze mondelinge beslissing wordt bevestigd door een met redenen omklede schriftelijke beslissing die de vermeldingen bedoeld in paragraaf 2 bevat, en die uiterlijk de eerste werkdag volgend op de datum van de beslissing moet toekomen op de zetel van de Commissie.	§ 3. In geval van hoogdringendheid kan het diensthoofd de specifieke methode mondeling toestaan. Deze mondelinge beslissing wordt bevestigd door een met redenen omklede schriftelijke beslissing die de vermeldingen bedoeld in paragraaf 2 bevat, en die uiterlijk de eerste werkdag volgend op de datum van de beslissing moet toekomen op de zetel van de Commissie.
De inlichtingenofficier kan mondeling of schriftelijk de medewerking vorderen van de personen bedoeld in de artikelen 18/6, 18/7 en 18/8. De aard van de methode wordt hen meegedeeld. Op een mondelinge vordering volgt zo spoedig mogelijk schriftelijke bevestiging ervan door de inlichtingenofficier.	**De methodenofficier** kan mondeling of schriftelijk de medewerking vorderen van de personen bedoeld in de artikelen 18/6, **18/6/1,** 18/7 en 18/8. De aard van de methode wordt hen meegedeeld. Op een mondelinge vordering volgt zo spoedig mogelijk schriftelijke bevestiging ervan door **de methodenofficier**.
§ 4. De specifieke methode kan enkel verlengd of hernieuwd worden mits een nieuwe beslissing van het diensthoofd, die voldoet aan de voorwaarden bepaald in § 1.	§ 4. De specifieke methode kan enkel verlengd of hernieuwd worden mits een nieuwe beslissing van het diensthoofd, die voldoet aan de voorwaarden bepaald in § 1.
§ 5. De specifieke methoden kunnen slechts worden aangewend ten opzichte van een advocaat, een arts of een journalist, of van communicatiemiddelen die ze voor beroepsdoeleinden gebruiken, op voorwaarde dat de inlichtingen- en veiligheidsdienst vooraf over ernstige aanwijzingen beschikt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of aan de ontwikkeling van de potentiële dreiging en nadat de commissie, overeenkomstig artikel 18/10 een eensluidend advies uitgebracht heeft op het ontwerp van beslissing van het diensthoofd.	§ 5. De specifieke methoden kunnen slechts worden aangewend ten opzichte van een advocaat, een arts of een journalist, of van communicatiemiddelen die ze voor beroepsdoeleinden gebruiken, op voorwaarde dat de inlichtingen- en veiligheidsdienst vooraf over ernstige aanwijzingen beschikt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of aan de ontwikkeling van de potentiële dreiging en nadat de commissie, overeenkomstig artikel 18/10 een eensluidend advies uitgebracht heeft op het ontwerp van beslissing van het diensthoofd.
§ 6. De leden van de commissie kunnen op elk ogenblik een controle uitoefenen op de wettigheid van de maatregelen, hierbij inbegrepen de naleving van de principes van subsidiariteit en proportionaliteit bepaald in artikel 18/9, § § 2 en 3.	§ 6. De leden van de commissie kunnen op elk ogenblik een controle uitoefenen op de wettigheid van de **specifieke methoden voor het verzamelen van gegevens, hierbij inbegrepen de naleving van de principes van subsidiariteit en proportionaliteit bepaald in artikel 18/3, §1**.
Zij kunnen daartoe de plaatsen betreden waar de gegevens betreffende de specifieke methode door de inlichtingen- en veiligheidsdiensten in ontvangst worden genomen of bewaard, zich alle nuttige stukken toe-eigenen en de leden van de dienst horen.	Zij kunnen daartoe de plaatsen betreden waar de gegevens betreffende de specifieke methode door de inlichtingen- en veiligheidsdiensten in ontvangst worden genomen of bewaard, zich alle nuttige stukken toe-eigenen en de leden van de dienst horen.

De gegevens verkregen in omstandigheden die de vigerende wettelijke bepalingen niet naleven, worden onder het toezicht van de Commissie bewaard overeenkomstig de door de Koning bepaalde nadere regels en termijnen, na advies van de commissie voor de bescherming van de persoonlijke levenssfeer. De commissie verbiedt de inlichtingen- en veiligheidsdiensten deze gegevens te exploiteren en schorst de aangewende methode indien deze nog lopende is.	De gegevens verkregen in omstandigheden die de vigerende wettelijke bepalingen niet naleven, worden onder het toezicht van de Commissie bewaard overeenkomstig de door de Koning bepaalde nadere regels en termijnen, na advies van **het Vast Comité I**. De commissie verbiedt de inlichtingen- en veiligheidsdiensten deze gegevens te exploiteren en schorst de aangewende methode indien deze nog lopende is.
De commissie stelt het Vast Comité I op eigen initiatief en onverwijld in kennis van haar beslissing.	De commissie stelt het Vast Comité I op eigen initiatief en onverwijld in kennis van haar beslissing.
§ 7 De inlichtingenofficier die is aangesteld om de aanwending van de specifieke methode voor het verzamelen van gegevens op te volgen, informeert het diensthoofd regelmatig over de uitvoering van deze methode.	§ 7 De **methodenofficier** die is aangesteld om de aanwending van de specifieke methode voor het verzamelen van gegevens op te volgen, informeert het diensthoofd regelmatig over de uitvoering van deze methode.
§ 8. Het diensthoofd beëindigt de specifieke methode wanneer de potentiële dreiging die haar rechtvaardigt weggevallen is, wanneer de methode niet langer nuttig is voor het doel waarvoor zij werd ingesteld, of wanneer hij een onwettigheid heeft vastgesteld. Hij brengt zijn beslissing zo spoedig mogelijk ter kennis van de Commissie.	§ 8. Het diensthoofd beëindigt de specifieke methode wanneer de potentiële dreiging die haar rechtvaardigt weggevallen is, wanneer de methode niet langer nuttig is voor het doel waarvoor zij werd ingesteld, of wanneer hij een onwettigheid heeft vastgesteld. Hij brengt zijn beslissing zo spoedig mogelijk ter kennis van de Commissie.
	Art. 18/5/1
	De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, in de virtuele wereld infiltreren onder dekmantel van een fictieve identiteit of fictieve hoedanigheid.
Art. 18/9	**Art. 18/9**
§ 1. De in artikel 18/2, § 2, bedoelde uitzonderlijke methoden voor het verzamelen van gegevens kunnen worden aangewend :	§ 1. De in artikel 18/2, § 2, bedoelde uitzonderlijke methoden voor het verzamelen van gegevens kunnen worden aangewend :
1° door de Veiligheid van de Staat, wanneer er een ernstige potentiële dreiging bestaat voor een fundamenteel belang van het land bedoeld in artikel 8, 2° tot 4°, en wanneer deze potentiële dreiging betrekking heeft op een	1° door de Veiligheid van de Staat, wanneer er een ernstige potentiële dreiging bestaat voor een fundamenteel belang van het land bedoeld in artikel 8, 2° tot 4°, en wanneer deze potentiële dreiging betrekking heeft op een activiteit bedoeld

activiteit bedoeld in artikel 8, 1° of verband houdt met een activiteit van een buitenlandse inlichtingendienst;	in artikel 8, 1° of verband houdt met een activiteit van een buitenlandse inlichtingendienst **of in het kader van artikel 18, § 2, indien er ernstig potentieel nadeel bestaat voor de uitoefening van de opdrachten van de diensten of een ernstig potentieel gevaar voor de veiligheid van de menselijke bron**;
2° door de Algemene Dienst Inlichting en Veiligheid wanneer er een ernstige potentiële dreiging bestaat voor een fundamenteel belang bedoeld in artikel 11, § 1, 1° tot 3° en 5°, met uitzondering van elk ander fundamenteel belang van het land bedoeld in artikel 11, § 1, 1°, f).	2° door de Algemene Dienst Inlichting en Veiligheid wanneer er een ernstige potentiële dreiging bestaat voor een fundamenteel belang bedoeld in artikel 11, § 1, 1° tot 3° en 5°, met uitzondering van elk ander fundamenteel belang van het land bedoeld in artikel 11, § 1, 1°, f) **of in het kader van artikel 18, § 2, indien er een ernstig potentieel nadeel bestaat voor de uitoefening van de opdrachten van de diensten of een ernstig potentieel gevaar voor de veiligheid van de menselijke bron.**
§ 2. Bij uitzondering en rekening houdend met een potentiële dreiging zoals bedoeld in paragraaf 1 kunnen de in artikel 18/2, § 2, bedoelde uitzonderlijke methoden voor het verzamelen van gegevens slechts aangewend worden indien de gewone en de specifieke methoden voor het verzamelen van gegevens ontoereikend worden geacht om de informatie te verzamelen die nodig is om de inlichtingenopdracht te volbrengen.	§ 2. Bij uitzondering en **rekening houdend met een potentiële dreiging, nadeel of gevaar zoals bedoeld in paragraaf 1** kunnen de in artikel 18/2, § 2, bedoelde uitzonderlijke methoden voor het verzamelen van gegevens slechts aangewend worden indien de gewone en de specifieke methoden voor het verzamelen van gegevens ontoereikend worden geacht om de informatie te verzamelen die nodig is om de inlichtingenopdracht te volbrengen.
Het diensthoofd mag de aanwending van een uitzonderlijke methode slechts machtigen na eensluidend advies van de commissie.	Het diensthoofd mag de aanwending van een uitzonderlijke methode slechts machtigen na eensluidend advies van de commissie.
§ 3. De uitzonderlijke methode moet worden gekozen in functie van de graad van de ernst van de potentiële dreiging.	§ 3. De uitzonderlijke methode moet worden gekozen in functie van de graad van de ernst van de potentiële dreiging **of in functie van de graad van de ernst van het potentieel nadeel voor de uitoefening van de opdrachten van de diensten of het potentiële gevaar voor de veiligheid van de menselijke bron in het kader van artikel 18 §2**.
§ 4. De uitzonderlijke methoden kunnen slechts aangewend worden ten opzichte van een advocaat, een arts of een journalist, of van hun lokalen of communicatiemiddelen die ze voor beroepsdoeleinden gebruiken, of van hun verblijfplaats, of van hun woonplaats, op voorwaarde dat de inlichtingen- en veiligheidsdienst vooraf over ernstige	§ 4. De uitzonderlijke methoden kunnen slechts aangewend worden ten opzichte van een advocaat, een arts of een journalist, of van hun lokalen of communicatiemiddelen die ze voor beroepsdoeleinden gebruiken, of van hun verblijfplaats, of van hun woonplaats, op voorwaarde dat de inlichtingen- en veiligheidsdienst vooraf over ernstige

aanwijzingen beschikt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of aan de ontwikkeling van een ernstige potentiële dreiging bedoeld in paragraaf 1.	aanwijzingen beschikt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of aan de ontwikkeling van een ernstige potentiële dreiging bedoeld in paragraaf 1.
Art. 18/10	**Art. 18/10**
§ 1. Het diensthoofd onderwerpt zijn ontwerp van machtiging aan het eensluidend advies van de commissie, die onderzoekt of de wettelijke bepalingen voor het aanwenden van de uitzonderlijke methode voor het verzamelen van gegevens, alsook de in artikel 18/9 § § 2 en 3, bepaalde principes van subsidiariteit en proportionaliteit, zijn nageleefd en die de door § 2 voorgeschreven vermeldingen controleert.	§ 1. Het diensthoofd onderwerpt zijn ontwerp van machtiging aan het eensluidend advies van de commissie, die onderzoekt of de wettelijke bepalingen voor het aanwenden van de uitzonderlijke methode voor het verzamelen van gegevens, alsook de in artikel 18/9 § § 2 en 3, bepaalde principes van subsidiariteit en proportionaliteit, zijn nageleefd en die de door § 2 voorgeschreven vermeldingen controleert.
Behoudens andersluidende wettelijke bepaling mag de periode tijdens welke de uitzonderlijke methode voor het verzamelen van gegevens aangewend mag worden niet langer duren dan twee maanden, te rekenen vanaf de machtiging, onverminderd de mogelijkheid om de methode te verlengen overeenkomstig § 5.	Behoudens andersluidende wettelijke bepaling mag de periode tijdens welke de uitzonderlijke methode voor het verzamelen van gegevens aangewend mag worden niet langer duren dan twee maanden, te rekenen vanaf de machtiging, onverminderd de mogelijkheid om de methode te verlengen overeenkomstig § 5.
De inlichtingenofficier die is aangesteld om de aanwending van de uitzonderlijke methode voor het verzamelen van gegevens op te volgen, informeert op regelmatige wijze het diensthoofd, dat op zijn beurt, overeenkomstig de door de Koning bepaalde nadere regels en termijnen, de commissie inlicht over de uitvoering van deze methode.	De **methodenofficier** die is aangesteld om de aanwending van de uitzonderlijke methode voor het verzamelen van gegevens op te volgen, informeert op regelmatige wijze het diensthoofd, dat op zijn beurt, overeenkomstig de door de Koning bepaalde nadere regels en termijnen, de commissie inlicht over de uitvoering van deze methode.
Het diensthoofd beëindigt de uitzonderlijke methode wanneer de ernstige potentiële dreiging die haar rechtvaardigt weggevallen is, wanneer de methode niet langer nuttig is voor het doel waarvoor zij werd ingesteld, of wanneer hij een onwettigheid heeft vastgesteld. Hij brengt zijn beslissing zo spoedig mogelijk ter kennis van de Commissie.	Het diensthoofd beëindigt de uitzonderlijke methode wanneer de ernstige potentiële dreiging die haar rechtvaardigt weggevallen is, wanneer de methode niet langer nuttig is voor het doel waarvoor zij werd ingesteld, of wanneer hij een onwettigheid heeft vastgesteld. Hij brengt zijn beslissing zo spoedig mogelijk ter kennis van de Commissie.
§ 2. Het ontwerp van machtiging van het diensthoofd vermeldt:	§ 2. Het ontwerp van machtiging van het diensthoofd vermeldt:
1° de aard van de uitzonderlijke methode;	1° de aard van de uitzonderlijke methode;
2° naargelang het geval, de natuurlijke personen of rechtspersonen, feitelijke	2° naargelang het geval, de natuurlijke personen of rechtspersonen, feitelijke verenigingen of

verenigingen of groeperingen, voorwerpen, plaatsen, gebeurtenissen of informatie die het voorwerp uitmaken van de uitzonderlijke methode;	groeperingen, voorwerpen, plaatsen, gebeurtenissen of informatie die het voorwerp uitmaken van de uitzonderlijke methode;
3° de ernstige potentiële dreiging die de uitzonderlijke methode voor het verzamelen van gegevens rechtvaardigt;	3° de ernstige potentiële dreiging die de uitzonderlijke methode voor het verzamelen van gegevens rechtvaardigt;
4° de feitelijke omstandigheden die de uitzonderlijke methode rechtvaardigen, de motivering inzake subsidiariteit en proportionaliteit, inbegrepen het verband tussen de bepalingen onder 2° en 3°;	4° de feitelijke omstandigheden die de uitzonderlijke methode rechtvaardigen, de motivering inzake subsidiariteit en proportionaliteit, inbegrepen het verband tussen de bepalingen onder 2° en 3°;
5° de periode waarin de uitzonderlijke methode voor het verzamelen van gegevens kan worden aangewend, te rekenen vanaf de machtiging van het diensthoofd;	5° de periode waarin de uitzonderlijke methode voor het verzamelen van gegevens kan worden aangewend, te rekenen vanaf de machtiging van het diensthoofd;
6° de naam van de inlichtingenofficier(en) verantwoordelijk om de aanwending van de uitzonderlijke methode op te volgen;	6° de naam van de **methodenofficier**(en) verantwoordelijk om de aanwending van de uitzonderlijke methode op te volgen;
7° in voorkomend geval, het technisch middel dat gebruikt wordt bij de aanwending van de uitzonderlijke methode in toepassing van de artikelen 18/11 of 18/12;	7° in voorkomend geval, het technisch middel dat gebruikt wordt bij de aanwending van de uitzonderlijke methode in toepassing van de artikelen 18/11 of 18/12;
8° in voorkomend geval, de samenloop met een opsporings- of gerechtelijk onderzoek;	8° in voorkomend geval, de samenloop met een opsporings- of gerechtelijk onderzoek;
9° in voorkomend geval, de strafbare feiten die strikt noodzakelijk zijn voor het welslagen van de uitvoering van de methode of ter verzekering van de veiligheid van de agenten of derden;	9° in voorkomend geval, **de feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd** die strikt noodzakelijk zijn voor het welslagen van de uitvoering van de methode of ter verzekering van de veiligheid van de agenten of derden;
10° in voorkomend geval, de ernstige aanwijzingen waaruit blijkt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of de ontwikkeling van de potentiële dreiging;	10° in voorkomend geval, de ernstige aanwijzingen waaruit blijkt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of de ontwikkeling van de potentiële dreiging;
11° in voorkomend geval, de redenen die de hoogdringendheid rechtvaardigen;	11° in voorkomend geval, de redenen die de hoogdringendheid rechtvaardigen;
12° de datum van de machtiging;	12° de datum van de machtiging;

13° de handtekening van het diensthoofd. De in het eerste lid bedoelde vermeldingen zijn op straffe van onwettigheid voorgeschreven.	13° de handtekening van het diensthoofd. De in het eerste lid bedoelde vermeldingen zijn op straffe van onwettigheid voorgeschreven.
	In het kader van artikel 18 §2 en in afwijking van paragraaf 2, 2° en 3°, vermeldt de beslissing van het diensthoofd respectievelijk de identificatiecode van de menselijke bron en het potentieel nadeel voor de uitoefening van de opdrachten van de diensten of het potentiële gevaar voor de veiligheid van de menselijke bron.
§ 3. De commissie verleent haar eensluidend advies binnen de vier dagen na ontvangst van het ontwerp van machtiging.	§ 3. De commissie verleent haar eensluidend advies binnen de vier dagen na ontvangst van het ontwerp van machtiging.
Indien de commissie een negatief advies uitbrengt, mag de uitzonderlijke methode voor het verzamelen van gegevens door de betrokken dienst niet worden aangewend.	Indien de commissie een negatief advies uitbrengt, mag de uitzonderlijke methode voor het verzamelen van gegevens door de betrokken dienst niet worden aangewend.
Indien de commissie geen advies uitbrengt binnen de termijn van vier dagen of zij de betrokken dienst meedeelt dat zij niet kan beraadslagen binnen die termijn overeenkomstig artikel 43, § 1, zevende lid, kan de betrokken dienst de bevoegde minister aanzoeken, die al dan niet toelating geeft om zo spoedig mogelijk de beoogde methode uit te voeren. De minister deelt zijn beslissing mee aan de voorzitters van de commissie en van het Vast Comité I.	Indien de commissie geen advies uitbrengt binnen de termijn van vier dagen of zij de betrokken dienst meedeelt dat zij niet kan beraadslagen binnen die termijn overeenkomstig artikel 43, § 1, zevende lid, kan de betrokken dienst de bevoegde minister aanzoeken, die al dan niet toelating geeft om zo spoedig mogelijk de beoogde methode uit te voeren. De minister deelt zijn beslissing mee aan de voorzitters van de commissie en van het Vast Comité I.
Het diensthoofd brengt de minister op de hoogte van de opvolging van de aldus toegelaten uitzonderlijke methode door hem op regelmatige tijdstippen, zoals vastgelegd door de minister in zijn toelating, een omstandig verslag uit te brengen over het verloop van de methode.	Het diensthoofd brengt de minister op de hoogte van de opvolging van de aldus toegelaten uitzonderlijke methode door hem op regelmatige tijdstippen, zoals vastgelegd door de minister in zijn toelating, een omstandig verslag uit te brengen over het verloop van de methode.
De betrokken minister beëindigt de uitzonderlijke methode die hij heeft toegestaan wanneer de potentiële dreiging die haar rechtvaardigt weggevallen is of wanneer de methode niet langer nuttig blijkt voor het doel waarvoor zij werd beslist. Hij schorst de methode indien hij een onwettigheid vaststelt. In dat geval brengt de betrokken minister zijn	De betrokken minister beëindigt de uitzonderlijke methode die hij heeft toegestaan wanneer de potentiële dreiging die haar rechtvaardigt weggevallen is of wanneer de methode niet langer nuttig blijkt voor het doel waarvoor zij werd beslist. Hij schorst de methode indien hij een onwettigheid vaststelt. In dat geval brengt de betrokken minister zijn met redenen omklede

met redenen omklede beslissing om de uitzonderlijke methode te beëindigen of te schorsen, naargelang het geval, onverwijld ter kennis van de commissie, het diensthoofd en het Vast Comité I.	beslissing om de uitzonderlijke methode te beëindigen of te schorsen, naargelang het geval, onverwijld ter kennis van de commissie, het diensthoofd en het Vast Comité I.
§ 4. In geval van hoogdringendheid en wanneer elk uitblijven van de machtiging van aard is om de belangen bedoeld in artikel 18/9 ernstig in het gedrang te brengen, kan het diensthoofd, nadat hij wegens de hoogdringendheid het mondeling eensluidend advies van de voorzitter van de Commissie heeft verkregen, de uitzonderlijke methode voor het verzamelen van gegevens mondeling machtigen voor ten hoogste vijf dagen.	§ 4. In geval van hoogdringendheid en wanneer elk uitblijven van de machtiging van aard is om de belangen bedoeld in artikel 18/9 ernstig in het gedrang te brengen, kan het diensthoofd, nadat hij wegens de hoogdringendheid het mondeling eensluidend advies van de voorzitter van de Commissie heeft verkregen, de uitzonderlijke methode voor het verzamelen van gegevens mondeling machtigen voor ten hoogste vijf dagen.
Indien de voorzitter van de Commissie niet bereikbaar is, kan het diensthoofd contact opnemen met een ander lid van de Commissie.	Indien de voorzitter van de Commissie niet bereikbaar is, kan het diensthoofd contact opnemen met een ander lid van de Commissie.
De voorzitter, of het andere gecontacteerde lid, brengt de overige leden van de Commissie onmiddellijk op de hoogte van zijn mondeling advies.	De voorzitter, of het andere gecontacteerde lid, brengt de overige leden van de Commissie onmiddellijk op de hoogte van zijn mondeling advies.
De inlichtingenofficier kan schriftelijk de medewerking vorderen van de personen bedoeld in de artikelen 18/14, 18/15, 18/16 en 18/17. De aard van de methode wordt hen meegedeeld. Deze vordering wordt zo spoedig mogelijk aan het diensthoofd meegedeeld.	De **methodenofficier** kan schriftelijk de medewerking vorderen van de personen bedoeld in de artikelen 18/14, 18/15, 18/16 en 18/17. De aard van de methode wordt hen meegedeeld. Deze vordering wordt zo spoedig mogelijk aan het diensthoofd meegedeeld.
Het diensthoofd geeft schriftelijke bevestiging van de mondelinge machtiging en geeft daarvan kennis aan de zetel van de Commissie, volgens de door de Koning vastgestelde nadere regels, ten laatste binnen de vierentwintig uur vanaf deze machtiging. Deze schriftelijke bevestiging bevat de in paragraaf 2 bedoelde vermeldingen.	Het diensthoofd geeft schriftelijke bevestiging van de mondelinge machtiging en geeft daarvan kennis aan de zetel van de Commissie, volgens de door de Koning vastgestelde nadere regels, ten laatste binnen de vierentwintig uur vanaf deze machtiging. Deze schriftelijke bevestiging bevat de in paragraaf 2 bedoelde vermeldingen.
In voorkomend geval vermeldt die bevestiging de redenen die de handhaving rechtvaardigen van de aanwending van de methode na de termijn van vijf dagen, zonder de twee maanden bedoeld in paragraaf 1, tweede lid, te boven te gaan. In dat geval geldt die	In voorkomend geval vermeldt die bevestiging de redenen die de handhaving rechtvaardigen van de aanwending van de methode na de termijn van vijf dagen, zonder de twee maanden bedoeld in paragraaf 1, tweede lid, te boven te gaan. In dat geval geldt die bevestiging als ontwerp van machtiging bedoeld in paragraaf 1.

bevestiging als ontwerp van machtiging bedoeld in paragraaf 1.	
In geval de noodzaak tot handhaving van de methode na de termijn van vijf dagen niet kon worden voorzien, of in uitzonderlijke gevallen, kan het diensthoofd de verlenging ervan machtigen volgens de procedure onder het eerste lid.	In geval de noodzaak tot handhaving van de methode na de termijn van vijf dagen niet kon worden voorzien, of in uitzonderlijke gevallen, kan het diensthoofd de verlenging ervan machtigen volgens de procedure onder het eerste lid.
Indien de voorzitter een mondeling negatief advies uitbrengt, mag de uitzonderlijke methode voor het verzamelen van gegevens door de betrokken dienst niet worden aangewend.	Indien de voorzitter **of het gecontacteerde Commissielid** een mondeling negatief advies uitbrengt, mag de uitzonderlijke methode voor het verzamelen van gegevens door de betrokken dienst niet worden aangewend.
Indien de voorzitter in geval van hoogdringendheid niet onmiddellijk advies uitbrengt, kan de betrokken dienst de bevoegde minister aanzoeken, die al dan niet de toelating geeft de beoogde methode uit te voeren. De minister deelt zijn beslissing mee aan de voorzitters van de commissie en van het Vast Comité I.	Indien de voorzitter **of het gecontacteerde Commissielid** in geval van hoogdringendheid niet onmiddellijk advies uitbrengt, kan de betrokken dienst de bevoegde minister aanzoeken, die al dan niet de toelating geeft de beoogde methode uit te voeren. De minister deelt zijn beslissing mee aan de voorzitters van de commissie en van het Vast Comité I.
Het diensthoofd brengt de minister op de hoogte van de opvolging van de aldus toegelaten uitzonderlijke methode door hem op regelmatige tijdstippen, zoals vastgelegd door de minister in zijn toelating, een omstandig verslag uit te brengen over het verloop van de methode.	Het diensthoofd brengt de minister op de hoogte van de opvolging van de aldus toegelaten uitzonderlijke methode door hem op regelmatige tijdstippen, zoals vastgelegd door de minister in zijn toelating, een omstandig verslag uit te brengen over het verloop van de methode.
De betrokken minister beëindigt de uitzonderlijke methode die hij heeft toegestaan wanneer de potentiële dreiging die haar rechtvaardigt weggevallen is of wanneer de methode niet langer nuttig blijkt voor het doel waarvoor zij werd beslist. Hij schorst de methode indien hij een onwettigheid vaststelt. In dat geval brengt de betrokken minister zijn met redenen omklede beslissing om de methode te beëindigen of te schorsen, naargelang het geval, onverwijld ter kennis van de commissie, het diensthoofd en het Vast Comité I.	De betrokken minister beëindigt de uitzonderlijke methode die hij heeft toegestaan wanneer de potentiële dreiging die haar rechtvaardigt weggevallen is of wanneer de methode niet langer nuttig blijkt voor het doel waarvoor zij werd beslist. Hij schorst de methode indien hij een onwettigheid vaststelt. In dat geval brengt de betrokken minister zijn met redenen omklede beslissing om de methode te beëindigen of te schorsen, naargelang het geval, onverwijld ter kennis van de commissie, het diensthoofd en het Vast Comité I.
In ieder geval wordt de uitzonderlijke methode stopgezet binnen vijf dagen na de door de betrokken minister verleende toelating,	In ieder geval wordt de uitzonderlijke methode stopgezet binnen vijf dagen na de door de betrokken minister verleende toelating, behalve in

behalve in de gevallen van verlenging bedoeld in het vijfde en zesde lid.	de gevallen van verlenging bedoeld in het vijfde en zesde lid.
§ 5. Het diensthoofd kan, op voorafgaand eensluidend advies van de commissie, de verlenging van de uitzonderlijke methode voor het verzamelen van gegevens machtigen voor een nieuwe termijn die niet langer mag zijn dan twee maanden te rekenen vanaf het verstrijken van de lopende methode, onverminderd zijn verplichting om de methode te beëindigen zodra de potentiële dreiging die haar rechtvaardigt weggevallen is, wanneer de methode niet langer nuttig is voor het doel waarvoor zij werd beslist of wanneer hij een onwettigheid vaststelt. In dat geval brengt het diensthoofd van de betrokken dienst zijn met redenen omklede beslissing om de methode te beëindigen ter kennis van de commissie.	§ 5. Het diensthoofd kan, op voorafgaand eensluidend advies van de commissie, de verlenging van de uitzonderlijke methode voor het verzamelen van gegevens machtigen voor een nieuwe termijn die niet langer mag zijn dan twee maanden te rekenen vanaf het verstrijken van de lopende methode, onverminderd zijn verplichting om de methode te beëindigen zodra de potentiële dreiging die haar rechtvaardigt weggevallen is, wanneer de methode niet langer nuttig is voor het doel waarvoor zij werd beslist of wanneer hij een onwettigheid vaststelt. In dat geval brengt het diensthoofd van de betrokken dienst zijn met redenen omklede beslissing om de methode te beëindigen ter kennis van de commissie.
Een tweede en elke volgende verlenging van de uitzonderlijke methode voor het verzamelen van gegevens is slechts mogelijk indien er bijzondere omstandigheden aanwezig zijn, die de verlenging van het gebruik van deze methode noodzaken. Deze bijzondere redenen worden in de beslissing opgenomen. Indien deze bijzondere omstandigheden niet voorhanden zijn, dient de methode te worden beëindigd.	Een tweede en elke volgende verlenging van de uitzonderlijke methode voor het verzamelen van gegevens is slechts mogelijk indien er bijzondere omstandigheden aanwezig zijn, die de verlenging van het gebruik van deze methode noodzaken. Deze bijzondere redenen worden in de beslissing opgenomen. Indien deze bijzondere omstandigheden niet voorhanden zijn, dient de methode te worden beëindigd.
De voorwaarden bepaald in de paragrafen 1 tot 3 zijn toepasselijk op de in deze paragraaf bepaalde wijzen van verlenging van de uitzonderlijke methode voor het verzamelen van gegevens.	De voorwaarden bepaald in de paragrafen 1 tot 3 zijn toepasselijk op de in deze paragraaf bepaalde wijzen van verlenging van de uitzonderlijke methode voor het verzamelen van gegevens.
§ 6. De leden van de commissie kunnen op elk ogenblik controle uitoefenen op de wettigheid van de uitzonderlijke methoden voor het verzamelen van gegevens, hierbij inbegrepen de naleving van de principes van subsidiariteit en proportionaliteit bepaald in artikel 18/9, § § 2 en 3.	§ 6. De leden van de commissie kunnen op elk ogenblik controle uitoefenen op de wettigheid van de uitzonderlijke methoden voor het verzamelen van gegevens, hierbij inbegrepen de naleving van de principes van subsidiariteit en proportionaliteit bepaald in artikel 18/9, § § 2 en 3.
Zij kunnen daartoe de plaatsen betreden waar de gegevens die met de uitzonderlijke methoden verzameld werden, in ontvangst genomen of bewaard worden, zich alle nuttige stukken toe-eigenen en de leden van de dienst horen.	Zij kunnen daartoe de plaatsen betreden waar de gegevens die met de uitzonderlijke methoden verzameld werden, in ontvangst genomen of bewaard worden, zich alle nuttige stukken toe-eigenen en de leden van de dienst horen.

De commissie beëindigt de uitzonderlijke methode voor het verzamelen van gegevens wanneer zij vaststelt dat de potentiële dreiging die haar rechtvaardigt weggevallen is of wanneer de uitzonderlijke methode niet meer nuttig blijkt te zijn voor het doel waarvoor ze werd aangewend, of schorst de uitzonderlijke methode ingeval van onwettigheid.	De commissie beëindigt de uitzonderlijke methode voor het verzamelen van gegevens wanneer zij vaststelt dat de potentiële dreiging die haar rechtvaardigt weggevallen is of wanneer de uitzonderlijke methode niet meer nuttig blijkt te zijn voor het doel waarvoor ze werd aangewend, of schorst de uitzonderlijke methode ingeval van onwettigheid.
De gegevens verkregen in omstandigheden die de vigerende wettelijke bepalingen niet naleven, worden onder het toezicht van de commissie bewaard overeenkomstig de door de Koning bepaalde regels en termijnen, na advies van de commissie voor de bescherming van de persoonlijke levenssfeer. De commissie verbiedt de inlichtingen- en veiligheidsdiensten deze gegevens te exploiteren.	De gegevens verkregen in omstandigheden die de vigerende wettelijke bepalingen niet naleven, worden onder het toezicht van de commissie bewaard overeenkomstig de door de Koning bepaalde regels en termijnen, na advies van **het Vast Comité I**. De commissie verbiedt de inlichtingen- en veiligheidsdiensten deze gegevens te exploiteren.
§ 7. De commissie stelt het Vast Comité I op eigen initiatief in kennis van het in § 2 bedoelde ontwerp van machtiging van de betrokken inlichtingen- en veiligheidsdienst, van het in § 3 bedoelde eensluidend advies, van de in paragraaf 4 bedoelde schriftelijke bevestiging van de mondelinge machtiging, van de in § 5 bedoelde eventuele verlenging van de uitzonderlijke methode voor het verzamelen van gegevens en van haar in § 6 bedoelde beslissing om de methode te beëindigen of in voorkomend geval te schorsen en de exploitatie van de aldus verzamelde gegevens te verbieden.	§ 7. De commissie stelt het Vast Comité I op eigen initiatief in kennis van het in § 2 bedoelde ontwerp van machtiging van de betrokken inlichtingen- en veiligheidsdienst, van het in § 3 bedoelde eensluidend advies, van de in paragraaf 4 bedoelde schriftelijke bevestiging van de mondelinge machtiging, van de in § 5 bedoelde eventuele verlenging van de uitzonderlijke methode voor het verzamelen van gegevens en van haar in § 6 bedoelde beslissing om de methode te beëindigen of in voorkomend geval te schorsen en de exploitatie van de aldus verzamelde gegevens te verbieden.
	Art. 18/12/1
	De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, in de reële wereld infiltreren, conform de richtlijnen van de Nationale Veiligheidsraad.
	Met reële wereld wordt bedoeld de relaties die hoofdzakelijk plaatsvinden via rechtstreekse fysieke contacten zonder dat daarbij zijn fysieke uiterlijk verborgen wordt.

	De methode is toegelaten zolang als nodig is voor het doel waarvoor ze wordt aangewend.
	De betrokken inlichtingen- en veiligheidsdienst brengt om de twee maanden verslag uit aan de Commissie over de evolutie van de dreiging die het beroep op een infiltratie in de reële wereld noodzakelijk maakte. Dit verslag benadrukt de elementen die hetzij het behoud, hetzij de stopzetting van de uitzonderlijke methode rechtvaardigen.
Art. 18/15	**Art. 18/15**
§ 1. In het belang van de uitoefening van hun opdrachten kunnen de inlichtingen- en veiligheidsdiensten de volgende gegevens vorderen :	**§ 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, informatie over de producten, diensten en verrichtingen van financiële aard en betreffende virtuele valuta, met betrekking tot de geviseerde persoon vorderen van:**
1° de lijst van bankrekeningen, bankkluizen of financiële instrumenten zoals bepaald in artikel 2, 1°, van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, waarvan de geviseerde persoon titularis, gevolmachtigde of de uiteindelijke gerechtigde is, en, in voorkomend geval, alle gegevens hieromtrent;	**1° de personen en instellingen bedoeld in artikel 5, paragraaf 1, 3° tot 22° van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;**
2° de bankverrichtingen die in een bepaald tijdvak zijn uitgevoerd op één of meer van deze bankrekeningen of financiële instrumenten, met inbegrip van de bijzonderheden betreffende iedere rekening van herkomst of bestemming;	**2° de personen en instellingen die, binnen het Belgisch grondgebied, diensten beschikbaar stellen of aanbieden met betrekking tot virtuele waarden die toelaten dat gereglementeerde betaalmiddelen in virtuele waarden worden uitgewisseld;**
3° de gegevens met betrekking tot de titularissen of gevolmachtigden die in een bepaald tijdvak tot deze bankkluizen toegang hebben of hadden.	**3° het Centraal Aanspreekpunt gehouden door de Nationale Bank van België overeenkomstig de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van bankrekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest.**
§ 2. De bank of de financiële instelling is ertoe gehouden de gevraagde informatie onverwijld te verstrekken aan een agent van de dienst, op vertoon van zijn legitimatiebewijs en een	**§2. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, van de personen en instellingen bedoeld in paragraaf 1, 1° en 2° vorderen dat de**

schriftelijke aanvraag van het diensthoofd. Deze vraag vermeldt, naargelang het geval, de aard van het eensluidend advies van de commissie, de aard van het eensluidend advies van de voorzitter van de commissie of de aard van de machtiging van de betrokken minister.	**verrichtingen van de geviseerde persoon onder toezicht worden geplaatst.**
De bank of de financiële instelling die de in dit artikel bedoelde medewerking weigert te verlenen, wordt gestraft met geldboete van zesentwintig euro tot twintigduizend euro.	**§ 3. De gevorderde medewerking bedoeld in paragraaf 1, 3° gebeurt overeenkomstig de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van bankrekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest.**
	De gevorderde persoon of instelling, bedoeld in paragraaf 1, 1° en 2°, is ertoe gehouden de gevraagde informatie onverwijld te verstrekken na ontvangst van de schriftelijke vordering van het diensthoofd.
	Deze vordering vermeldt, naargelang het geval, de aard van het eensluidend advies van de Commissie, de aard van het eensluidend advies van de voorzitter van de Commissie of de aard van de toelating van de betrokken minister. In deze vordering beschrijft de betrokken inlichtingen- en veiligheidsdienst eveneens nauwkeurig de informatie die wordt gevorderd en de vorm waarin deze wordt meegedeeld.
	§ 4. Iedere gevorderde persoon of instelling die de gegevens weigert mee te delen of niet meedeelt in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, wordt gestraft met gevangenisstraf van acht dagen tot een jaar en met geldboete van zesentwintig euro tot twintigduizend euro of met een van die straffen alleen.
Art. 20.	**Art. 20.**
§ 1. De inlichtingen- en veiligheidsdiensten, de politiediensten, de administratieve en gerechtelijke overheden zorgen voor een zo doeltreffend mogelijke wederzijdse samenwerking. De inlichtingen- en veiligheidsdiensten zorgen er eveneens voor dat er samenwerking is met de buitenlandse inlichtingen- en veiligheidsdiensten.	§ 1. De inlichtingen- en veiligheidsdiensten, de politiediensten, de administratieve en gerechtelijke overheden zorgen voor een zo doeltreffend mogelijke wederzijdse samenwerking. De inlichtingen- en veiligheidsdiensten zorgen er eveneens voor dat er samenwerking is met de buitenlandse inlichtingen- en veiligheidsdiensten.

§ 2. Wanneer ze daartoe door hen aangezocht worden kunnen de inlichtingen- en veiligheidsdiensten binnen de perken van een protocol goedgekeurd door de betrokken ministers hun medewerking en in het bijzonder hun technische bijstand verlenen aan de gerechtelijke en bestuurlijke overheden.	§ 2. Wanneer ze daartoe door hen aangezocht worden kunnen de inlichtingen- en veiligheidsdiensten hun medewerking en in het bijzonder hun technische bijstand verlenen aan de gerechtelijke en bestuurlijke overheden.
	De nadere regels voor deze medewerking kunnen in het kader van een protocol worden vastgelegd.
§ 3. de Nationale Veiligheidsraad bepaalt de in artikel 19, eerste lid, bedoelde voorwaarden waaronder de inlichtingen worden meegedeeld en de voorwaarden van de in § 1 van dit artikel bedoelde samenwerking.	§ 3. de Nationale Veiligheidsraad bepaalt de in artikel 19, eerste lid, bedoelde voorwaarden waaronder de inlichtingen worden meegedeeld en de voorwaarden van de in § 1 van dit artikel bedoelde samenwerking.
§ 4. Voor de opdrachten omschreven in artikel 7, 3°/1 en artikel 11, § 1, 5°, sluiten de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid, een samenwerkingsakkoord op grond van richtlijnen verkregen van de Nationale Veiligheidsraad.	§ 4. Voor de opdrachten omschreven in artikel 7, 3°/1 en artikel 11, § 1, 5°, sluiten de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid, een samenwerkingsakkoord op grond van richtlijnen verkregen van de Nationale Veiligheidsraad.

CHAMBRE • 4e SESSION DE LA 55e LÉGISLATURE 2021 2022 KAMER • 4e ZITTING VAN DE 55e ZITTINGSPERIODE

Imprimerie centrale – Centrale drukkerij