DOC 55 **2706/002**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

1er juillet 2022

PROJET DE LOI

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

RAPPORT

FAIT AU NOM DE LA COMMISSION
DE LA JUSTICE
PAR
M. **Koen GEENS**

SOMMAIRE Pages

Voir:

Doc 55 **2706/ (2021/2022)**:
001: Projet de loi.

Voir aussi:
003: Texte adopté par la commission.

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

1 juli 2022

WETSONTWERP

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

VERSLAG

NAMENS DE COMMISSIE
VOOR JUSTITIE
UITGEBRACHT DOOR
DE HEER **Koen GEENS**

INHOUD Blz.

Zie:

Doc 55 **2706/ (2021/2022)**:
001: Wetsontwerp.

Zie ook:
003: Tekst aangenomen door de commissie.

Composition de la commission à la date de dépôt du rapport/
Samenstelling van de commissie op de datum van indiening van het verslag
Président/Voorzitter: Kristien Van Vaerenbergh

A. — Titulaires / Vaste leden:		**B. — Suppléants / Plaatsvervangers:**
N-VA	Christoph D'Haese, Sophie De Wit, Kristien Van Vaerenbergh	Yngvild Ingels, Sander Loones, Wim Van der Donckt, Valerie Van Peel
Ecolo-Groen	Claire Hugon, Olivier Vajda, Stefaan Van Hecke	N ., Julie Chanson, Marie-Colline Leroy
PS	Khalil Aouasti, Laurence Zanchetta, Özlem Özen	N ., Mélissa Hanus, Ahmed Laaouej, Patrick Prévot
VB	Katleen Bury, Marijke Dillen	Tom Van Grieken, Dries Van Langenhove, Reccino Van Lommel
MR	Philippe Goffin, Philippe Pivin	Nathalie Gilson, Marie-Christine Marghem, Caroline Taquin
CD&V	Koen Geens	Els Van Hoof, Servais Verherstraeten
PVDA-PTB	Nabil Boukili	Greet Daems, Marco Van Hees
Open Vld	Katja Gabriëls	Patrick Dewael, Goedele Liekens
Vooruit	Ben Segers	Karin Jiroflée, Kris Verduyckt

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

Les Engagés	Vanessa Matz
DéFI	Sophie Rohonyi

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)*

MESDAMES, MESSIEURS,

Votre commission a examiné ce projet de loi au cours de ses réunions des 1er, 7 et 24 juin 2022. Les membres de la commission de la Défense ont également été invités à ces réunions.

I. — **PROCÉDURE**

Au cours de sa réunion du 7 juin 2022, la commission a décidé, en application de l'article 28.1 du Règlement de la Chambre, de recueillir des avis écrits, lesquels ont été mis à la disposition des membres.

II. — **EXPOSÉS INTRODUCTIFS**

A. **Exposé introductif du vice-premier ministre et ministre de la Justice et de la Mer du Nord**

M. Vincent Van Quickenborne, *vice-premier ministre et ministre de la Justice et de la Mer du Nord,* fait observer que le projet de loi à l'examen reprend un certain nombre de points d'un projet de son prédécesseur, M. Koen Geens.

Après les attentats terroristes du 22 mars 2016, la commission d'enquête parlementaire a constaté que la capacité d'information des services de renseignement devait être renforcée. Voici ce qu'en disait le rapport de la commission[1]:

"Les services de renseignement travaillent de préférence en faisant appel à l'human intelligence, ce qui est aussi leur force. Or, il est extrêmement difficile d'obtenir des sources humaines dans la communauté islamiste radicale, qui est très fermée. La commission d'enquête souhaite donc offrir aux services de renseignement des outils supplémentaires pour leur permettre de s'introduire dans cette communauté.

Les services doivent pouvoir mettre sur pied des opérations d'infiltration de longue durée. S'ils avaient davantage de moyens financiers, ils pourraient payer ces infiltrants. Un agent doit pouvoir obtenir rapidement une identité fictive sans que celle-ci doive être liée à une personne morale.

Certaines méthodes (comme les écoutes téléphoniques) qui, avant les attentats, ne pouvaient être

[1] *https://www.dekamer.be/kvvcr/pdf_sections/publications/attentats/Brochure_Terreuraanslagen.pdf*.

DAMES EN HEREN,

Uw commissie heeft dit wetsontwerp besproken tijdens haar vergaderingen van 1, 7 en 24 juni 2022. De leden van de commissie voor Defensie werden eveneens voor deze vergaderingen uitgenodigd.

I. — **PROCEDURE**

Tijdens haar vergadering van 7 juni 2022 heeft de commissie beslist om, met toepassing van artikel 28.1. van het Kamerreglement, schriftelijke adviezen in te winnen. De schriftelijke adviezen werden ter beschikking gesteld van de leden.

II. — **INLEIDENDE UITEENZETTINGEN**

A. **Inleidende uiteenzetting van de vice-eersteminister en minister van Justitie en Noordzee**

De heer Vincent Van Quickenborne, vice-eersteminister en minister van Justitie en Noordzee, merkt op dat het ter bespreking voorliggende wetsontwerp een aantal punten overneemt van een ontwerp van de vorige minister van Justitie, de heer Koen Geens.

Na de terroristische aanslagen van 22 maart 2016 stelde de parlementaire onderzoekscommissie vast dat de informatiepositie van de inlichtingendiensten versterkt moest worden. Het verslag ter zake vermeldt onder meer het volgende[1]:

"De inlichtingendiensten werken bij voorkeur met human intelligence, wat ook de sterkte van de diensten is. In de heel gesloten radicaal islamitische gemeenschap is het heel moeilijk om menselijke bronnen te werven. Daarom wil de onderzoekscommissie de inlichtingendiensten extra tools geven om zich in die gemeenschap in te werken.

De diensten moeten langdurige infiltratieoperaties kunnen opzetten. Met meer financiële middelen zouden ze zulke infiltranten kunnen betalen. Een agent moet vlot een fictieve identiteit kunnen krijgen, zonder dat dat gekoppeld moet zijn aan een rechtspersoon.

Bepaalde methoden (bijvoorbeeld telefoontap) die tot voor de aanslagen enkel op Belgisch grondgebied

[1] *https://www.dekamer.be/kvvcr/pdf_sections/publications/attentats/Brochure_Terreuraanslagen.pdf*.

appliquées que sur le territoire belge, devraient également pouvoir l'être lorsque la cible se trouve en dehors des frontières nationales.

Il faut développer une communication structurée systématique entre les services de renseignement et la police. C'est la seule façon de garantir que les informations cruciales seront toujours communiquées à tous les services concernés et donc de développer une approche intégrale du terrorisme islamiste.

L'accès aux canaux de communication des terroristes potentiels doit être optimisé. Il faut réclamer, au niveau européen et au niveau international, un accès aux applications de communication cryptée telles que WhatsApp. De même, l'exploitation des informations provenant des réseaux sociaux doit être professionnalisée.".

Le ministre attire l'attention sur le fait que l'accord de gouvernement, et donc sa politique, sont conformes à ces recommandations très importantes. Le problème de sous-effectif et de sous-financement de la VSSE sera réglé grâce à un renforcement significatif des services. Les échanges d'informations feront l'objet d'une rationalisation accrue dans le cadre d'un nouveau plan directeur du renseignement, sur lequel travaillent actuellement les services de la VSSE et du SGRS. La coordination des dossiers de terrorisme entre les services de renseignement, la police et le parquet sera également rationalisée au sein des *Joint Information Centers* et des *Joint Decision Centers*. La question de l'accès aux chats cryptés sera traitée dans le cadre de la conservation des données et fera également l'objet de discussions avec les instances européennes.

Le projet de loi à l'examen élimine certains obstacles légaux que les services rencontrent sur le terrain.

Le projet de loi permettra notamment:

— aux services de renseignement de s'infiltrer dans le monde virtuel ou dans le monde réel;

— aux agents de disposer de plus de possibilités de commettre des infractions dans le cadre de l'exercice de leurs fonctions (par exemple dans le cadre du travail des agents virtuels);

— et aux sources humaines de commettre des infractions moyennant le respect de conditions strictes;

mochten worden toegepast, zouden ook moeten worden toegepast als het target zich buiten de landsgrenzen bevindt.

Er moet een systematische en gestructureerde communicatie tussen de inlichtingendiensten en de politie worden uitgebouwd. Alleen zo kan cruciale informatie altijd op alle relevante diensten terechtkomen en kan er sprake zijn van een totaalaanpak van islamitisch terrorisme.

De toegang tot de communicatiekanalen van potentiële terroristen moet geoptimaliseerd worden. Op Europees en internationaal niveau moet gepleit worden om toegang te krijgen tot geëncrypteerde communicatie-applicaties zoals WhatsApp. Ook de exploitatie van info op sociale media moet worden geprofessionaliseerd.".

De minister vestigt er de aandacht op dat het regeerakkoord, en dus ook zijn beleid, enkele punten van deze erg belangrijke aanbevelingen afvinkt. Het probleem van de onderbezetting en van de onderfinanciering van de VSSE wordt aangepakt door de dienst fors te doen groeien. De informatie-uitwisseling wordt verder gestroomlijnd in een nieuw inlichtingenstuurplan tussen de VSSE en de ADIV dat momenteel tussen de diensten wordt uitgewerkt. De coördinatie van terrodossiers tussen inlichtingendiensten, politie en parket wordt ook verder gestroomlijnd in de *Joint Information Centers* en de *Joint Decision Centers*. Het punt over de toegang tot geëncrypteerde chats wordt behandeld in het dataretentiedossier en verder aangekaart met de Europese instanties.

Met dit wetsontwerp wordt beoogd een aantal van de wettelijke belemmeringen waar de diensten op het terrein tegenaan lopen weg te werken.

Het wetsontwerp voorziet onder meer in:

— de mogelijkheid voor de inlichtingendiensten om te infiltreren in de virtuele wereld of de reële wereld;

— een uitbreiding van de mogelijkheden voor agenten om tijdens de uitoefening van hun functie strafbare feiten te plegen (bijvoorbeeld in het kader van het werk van virtuele agenten);

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

— il permettra en outre d'appliquer les méthodes de recueil de données spécifiques (BIM) aux sources en vue de contrôler leur fiabilité, leur discrétion ou leur loyauté.

Il va de soi que les services de renseignement ne seront pas pour autant libres d'encourager le radicalisme mais ils pourront toutefois, par exemple, dans certaines circonstances, rendre un service à un terroriste potentiel afin de pouvoir conserver leur couverture. Cette méthode devra faire l'objet d'une autorisation préalable de la part de la commission BIM composée de trois magistrats qui devront valider *a priori* l'application de méthodes particulières de renseignement. Ces compétences avancées seront donc soumises à un contrôle avancé. Le Comité permanent R contrôlera également les services.

B. **Exposé introductif de Mme Ludivine Dedonder, ministre de la Défense**

Mme Ludivine Dedonder, ministre de la Défense, indique que le projet de loi à l'examen répond à une série d'attentes formulées par la commission d'enquête parlementaire sur les attentats et dans l'accord de gouvernement fédéral. Le projet de loi à l'examen s'inscrit dans le fil dudit rapport en ce sens qu'il vise à renforcer les services de renseignement belges. Les services de renseignement disposeront dès lors d'une série d'instruments supplémentaires pour recueillir des informations et ces instruments seront adaptés à la manière dont les menaces peuvent se manifester.

En ce qui concerne le Service Général du Renseignement et de la Sécurité (SGRS) en particulier, la ministre attire l'attention de la commission sur l'élargissement des possibilités dont ce service dispose pour réagir à une cyberattaque. Jusqu'à présent, le SGRS ne pouvait réagir à cette forme d'attaque que si elle visait des infrastructures militaires. Le service était habilité à identifier l'assaillant, à le neutraliser, voire à réagir en lançant sa propre cyberattaque si nécessaire.

L'adaptation en projet lui permettra d'intervenir également en cas de cyberattaque visant des systèmes informatiques et de communications non gérés par la Défense. La Défense et le SGRS avaient déjà pris cet engagement dans la Stratégie cybersécurité Belgique 2.0 approuvée en mai 2021 par le Conseil national de sécurité. Le projet de loi à l'examen vise à inscrire cet engagement dans la loi.

Cet engagement est parfaitement conforme à la conviction de la ministre que les investissements en matière de Défense doivent également profiter à l'ensemble de la nation. C'est particulièrement le cas en ce qui concerne les cybermenaces, qui s'étendent à de

— de mogelijkheid om de bijzondere methoden voor het verzamelen van gegevens (BIM's) uit te voeren op bronnen om hun betrouwbaarheid, discretie of loyaliteit te controleren.

De inlichtingendiensten krijgen hierbij uiteraard geen carte blanche om radicalisme uit te lokken, maar wel om in afgebakende omstandigheden bijvoorbeeld een dienst te verlenen aan een potentiële terrorist, om de zogeheten "cover" te kunnen ophouden. Deze methode moet vooraf het fiat krijgen van de BIM-commissie, bestaande uit drie magistraten die het gebruik van bijzondere inlichtingenmethodes *a priori* moeten machtigen. Verregaande bevoegdheden worden op die manier gekoppeld aan een verregaande controle. Ook het Vast Comité I kijkt mee over de schouder van de diensten.

B. **Inleidende uiteenzetting van mevrouw Ludivine Dedonder, minister van Defensie**

Mevrouw Ludivine Dedonder, minister van Defensie, stipt aan dat dit wetsontwerp tegemoetkomt aan een aantal verwachtingen van de parlementaire onderzoekscommissie aanslagen en aan het federaal regeerakkoord. Het ter bespreking voorliggende wetsontwerp sluit aan bij de strekking van het rapport: een versterking van de Belgische inlichtingendiensten. Aldus krijgen de beide inlichtingendiensten een aantal bijkomende instrumenten om informatie te verzamelen, op een manier die is aangepast aan de manier waarop dreigingen tot stand kunnen komen.

In het bijzonder wat de Algemene Dienst Inlichting en Veiligheid (ADIV) betreft, vestigt de minister de aandacht van de commissie op de uitbreiding van de mogelijkheid om te reageren op een cyberaanval. Tot nu kon de ADIV enkel reageren op een dergelijke aanval wanneer daarbij militaire infrastructuur werd aangevallen. De dienst had daarbij de wettelijke mogelijkheid om de aanvaller te identificeren, te neutraliseren en indien nodig zelfs te reageren met een eigen cyberaanval.

De ontworpen aanpassing zal het mogelijk maken dit ook te doen bij een cyberaanval op informatie- en verbindingssystemen die niet worden beheerd door de minister van Defensie. Defensie en de ADIV namen dit engagement al op zich in de Belgische Cybersecurity Strategy 2.0 die in mei 2021 werd goedgekeurd door de Nationale Veiligheidsraad. Dit wetsontwerp beoogt dit engagement wettelijk te verankeren.

Dit engagement ligt volledig in lijn met de overtuiging van de minister dat investeringen in defensie ook ten goede moeten komen van de natie in het algemeen. Dit is bij uitstek het geval bij de cyberdreiging die veelomvattend is en waar een goede samenwerking tussen de

nombreux domaines et nécessitent une bonne coopération entre les services de sécurité belges. Le SGRS et, par extension, le département de la Défense entendent jouer un rôle central dans ce domaine à l'avenir.

Toujours en ce qui concerne le renforcement de la position d'information des services de renseignement, le projet de loi à l'examen apporte une solution aux manquements constatés dans le prolongement de l'affaire Jürgen Conings. Il a alors été constaté que les informations obtenues par le SGRS dans le cadre d'enquêtes de sécurité ou de vérification de sécurité devaient pouvoir être mieux partagées au sein de ce service et avec d'autres services de sécurité belges. C'est la raison pour laquelle le projet de loi prévoit un cadre légal plus clair qui vise à assurer la transmission de ces informations.

Le projet de loi tire dès lors également les leçons de l'affaire Conings. Il s'agit seulement de l'une des mesures prises, comme l'approbation du plan directeur 2022 du SGRS et les investissements réalisés en attirant du personnel supplémentaire, cet effort devant également être poursuivi durant les mois et les années à venir.

La méthode existante de collecte de données auprès des banques et des institutions financières est revue afin de l'adapter à l'avènement des cryptomonnaies et de simplifier l'identification des numéros de compte – sans toutefois modifier l'accès aux soldes et aux transactions.

Enfin, le projet de loi à l'examen prévoit quelques modifications visant à améliorer le fonctionnement quotidien en pratique et à remédier à des oublis du passé.

La ministre conclut en indiquant que le texte a été soumis à l'avis du Collège des procureurs généraux, du Comité permanent R et de la Commission BIM et qu'il tient compte de leurs avis.

III. — **DISCUSSION GÉNÉRALE**

Mme Sophie De Wit (N-VA) fait observer que certains des avis reçus sont plutôt positifs mais que d'autres sont en revanche critiques sur certains points. Elle reviendra plus en détail sur ces critiques au cours de la discussion des articles.

Les services de renseignement jouent un rôle important dans l'appareil de sûreté de l'État. Les nombreux attentats terroristes qui ont frappé l'Europe il y a quelques années – et le nombre probablement encore

Belgische veiligheidsdiensten essentieel is. De ADIV en bij uitbreiding het departement Defensie willen hierin in de toekomst een centrale rol spelen.

Nog in het kader van het versterken van de informatiepositie van de inlichtingendiensten creëert het ter bespreking voorliggende wetsontwerp een oplossing voor een mankement dat naar boven is gekomen in de nasleep van de zaak-Jürgen Conings. Er werd namelijk vastgesteld dat informatie die beschikbaar was in het kader van veiligheidsonderzoeken of veiligheidsverificaties, uitgevoerd door de ADIV, beter moet kunnen worden gedeeld binnen de dienst en ook met andere Belgische veiligheidsdiensten. Het wetsontwerp voorziet daarom in een duidelijker wettelijk kader om deze informatiedoorstroming te waarborgen.

In het wetsontwerp worden derhalve ook de lessen getrokken uit de zaak-Conings. Dit is maar één van de genomen maatregelen, samen met de goedkeuring van het Stuurplan ADIV 2022 en de investeringen die zijn gedaan met het aantrekken van extra personeel, een inspanning die ook de komende maanden en jaren zal worden voortgezet.

De reeds bestaande methode voor het verzamelen van gegevens bij banken en financiële instellingen wordt herzien om deze aan te passen aan de opkomst van *cryptocurrency*, en ook om de identificatie van een rekeningnummer te vereenvoudigen – zonder weliswaar de toegang tot de saldi en transacties te wijzigen.

Ten slotte zijn er enkele wijzigingen om de dagelijkse werking in de praktijk te verbeteren of vergetelheden uit het verleden te corrigeren.

De minister besluit dat de tekst voor advies werd voorgelegd aan het College van procureurs-generaal, het Vast Comité I en de BIM-commissie en ook rekening houdt met deze adviezen.

III. — **ALGEMENE BESPREKING**

Mevrouw Sophie De Wit (N-VA) merkt op dat een aantal van de ontvangen adviezen eerder positief zijn, andere zijn dan weer op bepaalde punten kritisch. Zij zal hierop tijdens de artikelsgewijze bespreking dieper ingaan.

De inlichtingendiensten spelen een belangrijke rol in het veiligheidsapparaat. De golf van terroristische aanslagen in Europa van enkele jaren geleden – en wellicht het nog grotere aantal verijdelde aanslagen – toont aan

plus important d'attentats déjoués – indiquent que le travail de la Sûreté de l'État (VSSE) et du Service Général du Renseignement et de la Sécurité (SGRS) est essentiel pour garantir la liberté et la sécurité de tout un chacun. L'intervenante se félicite que l'importance de ces services soit bien comprise depuis la dernière législature et que l'on investisse à nouveau dans l'architecture de la sécurité.

Les services de renseignement doivent être en mesure d'intervenir adéquatement non seulement sur le plan budgétaire, mais aussi en ce qui concerne leurs compétences légales. S'il apparaît que certaines choses changent – l'intervenante pense par exemple au *darkweb* ou à de nouvelles méthodes de communication –, les services de sécurité doivent être dotés des outils nécessaires pour pouvoir (continuer à) lutter efficacement contre les menaces pour la sécurité. Le projet de loi à l'examen contient certainement des éléments positifs en ce sens, par exemple en prévoyant la possibilité légale d'organiser des opérations d'infiltration dans un milieu spécifique. Par conséquent, la membre se félicite que cette recommandation importante de la commission d'enquête parlementaire sur les attentats du 22 mars 2016 soit enfin mise en œuvre.

Dans le cadre de l'élargissement des compétences en matière d'enquêtes, il est cependant essentiel de prendre en compte que celles-ci doivent être exercées en accordant une attention suffisante au respect des principes de l'État de droit. En effet, les méthodes de renseignement peuvent avoir de très lourdes implications pour la vie privée et les autres droits et libertés fondamentaux des personnes qui en font l'objet. Il convient dès lors de prévoir les balises nécessaires à cet égard. S'agissant de la possibilité de procéder à des infiltrations, le projet de loi à l'examen prévoit le bon équilibre en tenant compte des avis rendus à ce propos. Il est positif que les suggestions de la commission BIM, du Collège des procureurs généraux et du Comité permanent R aient été suivies.

Il n'en a malheureusement pas été de même pour deux autres volets du projet de loi à l'examen, à savoir (1) la commission d'infractions par des sources humaines et (2) l'abaissement du niveau de classification des demandes de données financières au niveau "méthode ordinaire".

A. La commission d'infractions par des sources humaines

Cette possibilité est créée par l'insertion d'un article 13/1/1 dans la loi du 30 novembre 1998. La procédure prévue est identique à celle qui permet aux agents des services de renseignement de commettre des infractions. Dans les deux cas, il est donc question

dat het werk van de Veiligheid van de Staat (VSSE) en van de Algemene Dienst Inlichting en Veiligheid (ADIV) essentieel is om de vrijheid en veiligheid van eenieder te waarborgen. Gelukkig is dat inzicht er sedert vorige regeerperiode gekomen en wordt er opnieuw geïnvesteerd in de veiligheidsarchitectuur.

De inlichtingendiensten moeten de mogelijkheden krijgen om adequaat te kunnen optreden: niet alleen wat het budget, maar ook wat hun wettelijke bevoegdheden betreft. Als blijkt dat er zich bepaalde evoluties voordoen, en de spreekster denkt hierbij bijvoorbeeld aan het *darkweb* of aan nieuwe manieren om te communiceren, dan moeten de veiligheidsdiensten de *tools* krijgen om bedreigingen van de veiligheid performant te kunnen (blijven) bestrijden. In die zin bevat dit wetsontwerp zeker positieve elementen, zoals het invoeren van de wettelijke mogelijkheid om infiltratieoperaties op te zetten zodat in een bepaald milieu kan worden binnengedrongen. Het is dan ook een goede zaak dat deze belangrijke aanbeveling van de parlementaire onderzoekscommissie naar de aanslagen van 22 maart 2016 eindelijk wordt uitgevoerd.

Essentieel bij het uitbreiden van de onderzoeksbevoegdheden van de inlichtingendiensten is evenwel dat dit met voldoende aandacht voor de principes van de rechtsstaat gebeurt. Inlichtingenmethoden kunnen zeer sterk ingrijpen op de privacy en andere fundamentele rechten en vrijheden van de personen die eraan worden onderworpen. De nodige "*checks and balances*" moeten dan ook worden gedaan. Wat de mogelijkheid tot infiltraties betreft, voorziet het wetsontwerp in het juiste evenwicht door rekening te houden met de adviezen die daarover werden afgeleverd. Het is positief dat de suggesties van de BIM-commissie, het College van procureurs-generaal en het Vast Comité I op dit vlak werden gevolgd.

Helaas is dit niet gebeurd voor twee andere onderdelen van het wetsontwerp, namelijk (1) het plegen van strafbare feiten door menselijke bronnen en (2) het opvragen van financiële gegevens die in dezen worden gereduceerd tot een "gewone methode".

A. Het plegen van strafbare feiten door menselijke bronnen

Deze mogelijkheid wordt gecreëerd door de invoeging van een nieuw artikel 13/1/1 in de wet van 30 november 1998. Het gaat om identiek dezelfde procedure als deze waarin is voorzien voor de mogelijkheid tot het plegen van strafbare feiten door agenten van de inlichtingendiensten.

de mesures très intrusives, surtout en ce qui concerne les sources humaines. En effet, on laisse un “citoyen ordinaire” infiltrer un certain milieu tout en l’autorisant à commettre des infractions si celles-ci s’avèrent nécessaires à la préservation de sa position d’information. La situation est différente pour un agent, dès lors qu’il a suivi une formation professionnelle à cette fin et qu’il est habitué à opérer dans des circonstances très difficiles. Il ne serait donc pas tout à fait logique d’appliquer une procédure et un mécanisme de contrôle identiques à ces deux cas de figure. Pour les sources humaines, il conviendrait tout de même de prévoir le mécanisme de contrôle le plus strict possible.

En outre, la commission BIM, le Collège des procureurs généraux et le Comité permanent R font à juste titre le parallèle avec l’infiltration civile prévue dans le Code pénal. Or, les mécanismes de contrôle et d’accompagnement applicables à l’infiltration civile sont nettement plus stricts que ceux applicables aux sources humaines. Le groupe N-VA souscrit dès lors à leur plaidoyer en faveur d’une classification comme méthode exceptionnelle de la possibilité d’autoriser des sources humaines à commettre des infractions.

B. La demande de données financières sera considérée comme une méthode ordinaire et non plus exceptionnelle

La collecte de données bancaires et financières a bel et bien une incidence sur la vie privée des personnes concernées par ces données et n’est pas aussi évidente que le présente le projet de loi à l’examen. En effet, comme l’indiquent aussi la commission BIM et le Comité permanent R, des informations importantes peuvent déjà être inférées de ces données. L’intervenante ne comprend donc pas pourquoi cette compétence d’enquête sera catégorisée comme une méthode ordinaire, et plus comme une méthode exceptionnelle.

Compte tenu des observations susmentionnées, la membre indique que son groupe s’abstiendra lors du vote sur l’ensemble du projet de loi à l’examen.

M. Stefaan Van Hecke (Ecolo-Groen) se réfère à la discussion qui s’est tenue, lors de la dernière réunion, au sujet des avis qui ont été demandés et reçus et il apprécie le degré de précision de l’avis du Comité R, qui a analysé le projet de loi en détail et formulé pas moins de 81 remarques. Il trouve cet exercice important et estime que chacune de ces remarques doit être discutée, de manière à ce qu’une justification suffisante soit donnée si elle n’est pas prise en compte dans le texte. Selon lui, la plupart des remarques ont donné lieu à des adaptations du texte, à juste titre. Il souligne par ailleurs qu’il était essentiel, dans ce processus, de

In beide gevallen gaat het dus over zeer ingrijpende maatregelen, zeker voor menselijke bronnen. Men laat immers een gewone burger infiltreren binnen een bepaald milieu, waarbij hij de toelating krijgt om indien noodzakelijk teneinde zijn informatiepositie veilig te stellen, een misdrijf te plegen. Voor een agent ligt dit anders, want die werd hiervoor professioneel opgeleid en is het gewend om in zeer moeilijke omstandigheden te werken. Het is dan ook niet zo logisch dat in beide gevallen identiek dezelfde procedure en controlemechanisme gelden. Voor menselijke bronnen zou toch in de meest strikte controle moeten worden voorzien.

De BIM-commissie, het College van procureurs-generaal en het Vast Comité I trekken bovendien terecht ook de parallel met de burgerinfiltratie uit het strafrecht. De controle- en begeleidingsmechanismen voor de burgerinfiltratie zijn evenwel een stuk strenger dan deze die bepaald zijn voor de menselijke bronnen. De N-VA-fractie onderschrijft dan ook hun pleidooi dat de mogelijkheid tot machtiging voor het plegen van strafbare feiten gepleegd door menselijke bronnen moet worden ingedeeld als een uitzonderlijke methode.

B. Het opvragen van financiële gegevens wordt een gewone methode in plaats van een uitzonderlijke methode

Het inwinnen van gegevens bij banken en financiële gegevens heeft wel degelijk een impact op de privacy van personen en is niet zo vanzelfsprekend als in het wetsontwerp wordt voorgesteld. Zoals de BIM-commissie en het Vast Comité I ook stellen, kan hieruit al belangrijke informatie worden afgeleid. De spreekster begrijpt dan ook niet dat deze onderzoeksbevoegdheid wordt gereduceerd tot een gewone methode in plaats van een uitzonderlijke methode.

Gelet op deze bedenkingen geeft het lid mee dat haar fractie zich bij de stemming over het geheel zal onthouden.

De heer Stefaan Van Hecke (Ecolo-Groen) verwijst naar het debat dat zich tijdens de jongste vergadering ontsponnen heeft over de aangevraagde en inmiddels ontvangen adviezen; hij waardeert met name de nauwkeurigheid van het advies van het Vast Comité I, dat het wetsontwerp grondig ontleed heeft en liefst 81 opmerkingen geformuleerd heeft. Hij vindt dit een belangrijke oefening en stelt dat elke opmerking besproken moet worden, zodat een toereikende verantwoording mogelijk is, mocht worden beslist in de tekst geen rekening te houden met deze of gene opmerking. Volgens hem hebben de meeste opmerkingen terecht geleid tot een

donner cet espace aux acteurs sur le terrain en leur permettant d'apporter leur contribution.

Il a entendu Mme De Wit lorsqu'elle a soulevé la nécessité, pour mettre en œuvre des mesures de ce type, de chercher un équilibre entre différents droits fondamentaux. Il se réjouit de constater qu'elle reconnaît que cet équilibre existe aussi au niveau global.

M. Van Hecke explique que le projet de loi prévoit trois niveaux de contrôle pour autoriser la commission d'infractions. Tout d'abord, une procédure interne, selon laquelle l'intervention de l'agent est validée par la hiérarchie. Deuxièmement, la Commission BIM doit donner son accord. Cette commission BIM est connue, il s'agit de trois magistrats qui doivent émettre un jugement dans un délai fixé, avec un rapport à la clé. Enfin, le Comité permanent R exerce lui aussi un contrôle. Il souligne que les recommandations qui ont été formulées par la commission d'enquête "Attentats terroristes" insistaient beaucoup sur l'importance de mettre en place des mécanismes de contrôle suffisants. Il estime que le mécanisme de contrôle prévu dans le présent projet de loi est suffisamment solide pour éviter les abus autant que possible et empêcher toute sortie de route.

M. Koen Geens (CD&V) se réjouit que le présent projet de loi soit à l'examen car il doit permettre aux personnes qui travaillent sur le terrain de mener à bien leur mission en toute sécurité. Il souligne que cette modification de la loi avait déjà été abordée en 2015 mais qu'elle n'avait pas pu être prise en compte lors de la grande réforme de la législation BIM en 2017, alors que la commission d'enquête "Attentats terroristes" avait conclu à la nécessité d'une telle adaptation. Le présent projet de loi se réfère, à juste titre, à l'arrêt de la Cour constitutionnelle du 22 avril 2021 (n° 64/2021), selon lequel la mise en œuvre de ce type de moyens de contrôle et d'enquête a pour finalité la sécurité de l'État, et non la lutte contre la criminalité.

Il souhaite tout d'abord savoir de quelle manière le motif d'exclusion de la culpabilité est communiqué à la police locale, concrètement, par exemple dans le cas où elle prend un agent ou une source humaine en flagrant délit et place cette personne en détention préventive.

M. Geens se réfère ensuite à l'arrêt du 21 juin de la Cour de Justice européenne concernant la législation PNR, en réponse à une question préjudicielle de la Belgique, et se demande si le ministre a eu le temps de vérifier si cet arrêt a un impact sur le présent projet de loi.

aanpassing van de tekst. Ook vond hij het belangrijk dat in dit proces ruimte werd gelaten voor de actoren in het veld, die hun bijdrage hebben kunnen leveren.

Hij heeft mevrouw De Wit horen benadrukken hoe noodzakelijk het is een balans tussen verschillende grondrechten te vinden alvorens dergelijke maatregelen ten uitvoer te leggen. Het verheugt hem dat zij beaamt dat dit evenwicht er over het algemeen ook is.

De heer Van Hecke geeft aan dat het wetsontwerp in drie controleniveaus voorziet om het plegen van strafbare feiten toe te staan. In de eerste plaats is er een interne procedure, waarbij de interventie van de agent goedgekeurd wordt door de hiërarchie. Ten tweede is de instemming van de BIM-commissie vereist. Die BIM-commissie is gekend; drie magistraten moeten binnen een welbepaalde termijn een beslissing nemen, aan de hand van een verslag. Tot slot oefent ook het Vast Comité I toezicht uit. Hij benadrukt dat de onderzoekscommissie naar de terroristische aanslagen in haar aanbevelingen erop heeft gehamerd dat het belangrijk is toereikende controlemechanismen in te stellen. Volgens hem is het in dit wetsontwerp ingebouwde controlemechanisme stevig genoeg om misbruik zoveel mogelijk te voorkomen en eventuele ontsporingen tegen te gaan.

De heer Koen Geens (CD&V) is ermee ingenomen dat dit wetsontwerp ter bespreking voorligt, want het moet ervoor zorgen dat de mensen in het veld hun werk in alle veiligheid kunnen doen. Hij benadrukt dat deze wetswijziging al in 2015 op de sporen gezet werd maar niet kon worden meegenomen in de brede hervorming van de BIM-wetgeving in 2017, terwijl de onderzoekscommissie naar de terroristische aanslagen geconcludeerd had dat een dergelijke aanpassing er diende te komen. Dit wetsontwerp verwijst terecht naar het arrest van het Grondwettelijk Hof van 22 april 2021 (nr. 64/2021), volgens hetwelk de tenuitvoerlegging van dit soort van controle- en onderzoeksmiddelen de veiligheid van de Staat en niet de strijd tegen de criminaliteit tot doel heeft.

Vooreerst wil hij weten hoe de uitsluitingsgrond voor de schuldvraag concreet aan de lokale politie wordt meegedeeld, bijvoorbeeld wanneer die een agent of een menselijke bron op heterdaad betrapt en de betrokkene in voorlopige hechtenis neemt.

Vervolgens verwijst de heer Geens naar het arrest van 21 juni 2022 van het Hof van Justitie van de EU over de PNR-wetgeving, als antwoord op een prejudiciële vraag van België; hij vraagt zich af of de minister al heeft kunnen nagaan of dat arrest een invloed op dit wetsontwerp heeft.

Le ministre de la Justice explique que le temps nécessaire a été pris pour rédiger ce projet de loi de la meilleure manière qui soit, avec l'aide de différentes instances, car il s'agit d'un dossier très délicat. Il répond à plusieurs recommandations de la commission d'enquête parlementaire et a fait l'objet d'avis très détaillés des différentes instances sollicitées.

En ce qui concerne la Sûreté de l'État, le mécanisme proposé réside selon lui en trois méthodes de recueil des données (BIM). La première, baptisée "*Human Intelligence*", consiste à travailler avec des sources humaines et à leur donner la possibilité de commettre des infractions, à des conditions très strictes et sous la supervision du Comité R. "Humint" n'est pas nouvelle; seule la possibilité, pour ces sources humaines, de commettre des infractions est nouvelle et elle répond à une demande expresse de la commission d'enquête. L'autorisation préalable de la commission BIM est une condition incontournable.

La deuxième méthode consiste à offrir davantage de modes d'intervention aux agents de la sûreté de l'État. Ces agents peuvent ainsi s'infiltrer tant dans le monde réel que virtuel, mais prennent bien entendu plus de risques dans le monde réel que dans le virtuel, étant donné leur présence physique sur les lieux. Ils peuvent par ailleurs s'infiltrer avec ou sans identité fictive. Enfin, ils peuvent commettre une infraction. Toutes ces modalités sont bien entendu soumises à des conditions strictes. S'il est question, par exemple, d'une infiltration dans le monde virtuel avec identité fictive, il s'agit d'une méthode spécifique qui doit faire l'objet d'un rapport *post factum* à la commission BIM. Si l'infiltration a lieu dans le monde réel, il est question d'une méthode exceptionnelle, pour laquelle l'accord de la commission BIM doit être donné au préalable. En effet, dans le monde réel, la personne court plus de risques que dans le monde virtuel. Si une identité fictive est utilisée, autrement dit que la personne se fait passer pour quelqu'un d'autre, cette identité doit pouvoir être prouvée avec un document pour ne pas courir de risque; ce n'est pas le cas, par exemple, avec un faux nom, qui sera plus facile à utiliser dans le monde virtuel. Pour utiliser une identité fictive, un registre est tenu qui est contrôlé par le Comité permanent R. Enfin, pour la commission d'une infraction, il faut aussi un accord préalable de la commission BIM. L'adaptation du texte, avec le recours systématique à la commission BIM, répond aux recommandations du Collège des procureurs généraux.

De minister van Justitie legt uit dat de nodige tijd werd genomen om dit wetsontwerp zo doordacht mogelijk op te stellen. Aangezien het om een heel gevoelig dossier gaat, werd daarbij een beroep gedaan op verschillende instanties. Het wetsontwerp beantwoordt aan meerdere aanbevelingen van de parlementaire onderzoekscommissie en de verschillende aangezochte instanties hebben er heel gedetailleerde adviezen over uitgebracht.

Wat de Veiligheid van de Staat betreft, berust de voorgestelde regeling volgens de minister op drie methoden voor het verzamelen van gegevens (BIM). De eerste, die "*Human Intelligence*" werd gedoopt, houdt in dat men samenwerkt met menselijke bronnen die onder heel strikte voorwaarden en onder het toezicht van het Vast Comité I strafbare feiten mogen plegen. "Humint" is geen nieuwe methode; het enige wat nieuw is, is het feit dat die menselijke bronnen strafbare feiten mogen plegen, waarmee gevolg wordt gegeven aan een uitdrukkelijk verzoek van de onderzoekscommissie. De voorafgaande toestemming van de BIM-commissie is een voorwaarde waar men niet omheen kan.

De tweede methode houdt in dat de agenten van de Veiligheid van de Staat meer mogelijkheden zullen krijgen om op te treden. Die agenten zullen bijvoorbeeld zowel in de echte als de virtuele wereld mogen infiltreren. In de echte wereld is het risico uiteraard groter, gezien hun fysieke aanwezigheid ter plekke. Voorts mogen ze infiltreren met of zonder fictieve identiteit. Ten slotte mogen ze een strafbaar feit plegen. Al die werkwijzen zijn uiteraard aan strikte voorwaarden onderworpen. Zo geldt infiltratie in de virtuele wereld met fictieve identiteit als een specifieke methode waarbij *post factum* aan de BIM-commissie moet worden gerapporteerd. Infiltratie in de echte wereld geldt als een uitzonderlijke methode, waarvoor men op voorhand de toestemming van de BIM-commissie moet krijgen. In de echte wereld loopt de betrokkene immers meer risico's dan in de virtuele wereld. Indien een fictieve identiteit wordt gebruikt – de betrokkene geeft zich met andere woorden uit voor iemand anders – moet die identiteit aan de hand van een document kunnen worden bewezen, opdat men geen risico loopt; dat is niet het geval met bijvoorbeeld een valse naam, die makkelijker kan worden gebruikt in de virtuele wereld. Om een fictieve identiteit te gebruiken, wordt een register bijgehouden dat wordt gecontroleerd door het Vast Comite I. Ten slotte is de voorafgaande toestemming van de BIM-commissie ook vereist om een strafbaar feit te mogen plegen. Bij de totstandkoming van het wetsontwerp, waarbij stelselmatig een beroep werd gedaan op de BIM-commissie, werd rekening gehouden met de aanbevelingen van het College van procureurs-generaal.

La troisième méthode concerne la récolte de données (BIM) sur la source. Lorsqu'il est fait appel à une source humaine, il faut pouvoir s'assurer de sa fiabilité. Il peut par exemple être nécessaire d'examiner des conversations ou des données téléphoniques pour vérifier que la source humaine ne révèle pas certaines informations à un tiers. Ou au contraire, cette récolte de données peut être nécessaire pour protéger la source, par exemple pour s'assurer que la couverture d'une source infiltrée dans un milieu radical n'est pas menacée. Cette méthode BIM peut être spécifique, par exemple par la récolte de métadonnées ou en prenant la personne en filature; dans ce cas, la validation doit se faire après le recueil des données. Et la méthode peut aussi être exceptionnelle, par exemple si la source doit être mise sur écoute, auquel cas il faut un accord préalable de la commission BIM.

Ce sont ces trois méthodes qu'il est question d'intégrer dans la loi de 1998, avec un élément supplémentaire: la problématique des comptes bancaires. Il est question d'adapter la législation à ce sujet. La récolte de données d'identification – qui se cache derrière un compte bancaire, par exemple, ou à qui appartient tel compte – devient une méthode ordinaire, alors qu'il s'agissait auparavant d'une méthode exceptionnelle. Par contre, la vérification du contenu d'un compte bancaire, des transactions et des soldes qui s'y rapportent, reste une méthode exceptionnelle.

L'avis du Collège des procureurs-généraux n'a pas été suivi sur un point. Pour le Collège, le système de sources humaines consiste en de l'infiltration citoyenne, pour laquelle une autorisation préalable du juge d'instruction est nécessaire. Or, le ministre considère que la méthode de la source humaine, qui est déjà utilisée depuis longtemps par la Sûreté de l'État, est d'ores et déjà soumise à des conditions très strictes, qu'il n'est pas nécessaire de renforcer: notes d'approche, rapports d'information, supervision du Comité permanent R.

En ce qui concerne la distinction de traitement entre les sources humaines et les agents, le ministre considère qu'il est normal que les procédures ne soient pas les mêmes. Pour les infractions commises par une source humaine, un accord préalable de la commission BIM est toujours requis, ainsi qu'une analyse de risques et une description détaillée de la personnalité et de la fiabilité de la source. Pour une infraction commise par un agent, il faut aussi un accord préalable de la commission BIM, sauf que l'agent peut, en cas d'extrême urgence, commettre une infraction sans accord préalable, et obtenir un accord *a posteriori*. Une infraction ne peut être commise de cette manière que pour sauvegarder

De derde methode betreft het verzamelen van gegevens (BIM) over een bron. Wanneer een beroep wordt gedaan op een menselijke bron, moet de betrouwbaarheid ervan kunnen worden gewaarborgd. Zo kan het nodig zijn telefoongesprekken of -gegevens te onderzoeken om na te gaan of de menselijke bron bepaalde informatie niet onthult aan een derde. Omgekeerd kan het verzamelen van gegevens ook nodig zijn om de bron te beschermen, om zich er bijvoorbeeld van te vergewissen dat de dekking van een bron die in een radicaal milieu is geïnfiltreerd niet bedreigd is. Die BIM-methode kan specifiek zijn, bijvoorbeeld bij het verzamelen van metagegevens of wanneer iemand wordt geschaduwd; in dat geval moet de validatie gebeuren na het verzamelen van de gegevens. De methode kan ook uitzonderlijk zijn, bijvoorbeeld wanneer de bron moet worden afgeluisterd. In dat geval is de voorafgaande toestemming van de BIM-commissie nodig.

Het is de bedoeling deze drie methodes op te nemen in de wet van 1998, met een bijkomend element: het vraagstuk van de bankrekeningen. De wetgeving zou op dat punt worden aangepast. De verzameling van identificatiegegevens – wie zit er bijvoorbeeld achter een bankrekening of wie is de eigenaar van een rekening – wordt een gewone methode, terwijl dit vroeger een uitzonderlijke methode was. De verificatie van de inhoud, de transacties en de saldi van een bankrekening blijft daarentegen een uitzonderlijke methode.

Het advies van het College van procureurs-generaal werd op één punt niet gevolgd. Het College meent dat de regeling inzake de menselijke bronnen burgerinfiltratie behelst, waarvoor de voorafgaande toestemming van de onderzoeksrechter is vereist. De minister daarentegen meent dat het werken met menselijke bronnen, een methode die reeds lang wordt toegepast door de Veiligheid van de Staat, nu al onderworpen is aan zeer strikte voorwaarden die niet moeten worden aangescherpt: benaderingsnota's, informatieverslagen, toezicht door het Vast Comité I.

Wat het verschil in behandeling betreft tussen de menselijke bronnen en de agenten, acht de minister het normaal dat de procedures verschillen. Voor de strafbare feiten begaan door een menselijke bron is steeds een voorafgaand akkoord van de BIM-commissie vereist, alsook een risicoanalyse en een gedetailleerde beschrijving van de persoonlijkheid en de betrouwbaarheid van de bron. Voor een strafbaar feit begaan door een agent is eveneens een voorafgaand akkoord van de BIM-commissie vereist, zij het dat de agent, in geval van hoogdringendheid, een strafbaar feit mag begaan zonder voorafgaand akkoord en *a posteriori* een akkoord kan krijgen. Een strafbaar feit mag enkel op die

la couverture de l'agent. Dans tous les cas, l'infraction doit être proportionnelle à la menace et elle ne peut pas porter atteinte à l'intégrité physique des personnes.

Le ministre souligne par ailleurs que la Sûreté de l'État est en train d'être renforcée. Au début de la législature, elle employait 580 collaborateurs, ce nombre s'élève maintenant à 747 et l'objectif est d'atteindre le millier de collaborateurs.

En réponse à la question sur la manière dont la police locale est informée, le ministre explique que la police n'est pas informée directement. Le parquet est contacté afin de discuter de la question en détail, de manière à ce que les informations soient transmises au moment opportun. Les exemptions de peine ressortissent d'ailleurs au parquet.

La ministre de la Défense précise que l'arrêt PNR a été rendu il y quelques jours, qu'il est en cours d'analyse et que des adaptations législatives seront encore apportées si nécessaire.

IV. — **DISCUSSION DES ARTICLES ET VOTES**

Art. 1er

Cet article fixe le fondement constitutionnel de la compétence.

L'article 1er est adopté à l'unanimité.

Art. 2

Cet article ne donne lieu à aucune observation.

L'article 2 est adopté à l'unanimité.

Art. 3

Cet article vise à modifier l'article 11 de la loi organique des services de renseignement et de sécurité du 30 novembre 1998.

Mme Sophie De Wit (N-VA) constate que cet article constitue la base légale permettant au SGRS de se mettre au service de la Nation en cas de crise nationale de cybersécurité. Or, l'exposé des motifs ne comporte guère d'arguments exposant la raison pour laquelle cette mission a été confiée au SGRS. En effet, il ne sera

manier worden begaan om de dekmantel van de agent te beschermen. In alle gevallen moet het strafbaar feit in verhouding staan tot de dreiging en mag het geen afbreuk doen aan de fysieke integriteit van personen.

De minister benadrukt bovendien dat de Veiligheid van de Staat momenteel wordt uitgebouwd. Bij de aanvang van de regeerperiode telde die instantie 580 medewerkers; momenteel zijn het er 747 en het is de bedoeling dat het er uiteindelijk 1 000 zullen zijn.

Als antwoord op de vraag hoe de lokale politie wordt geïnformeerd, stelt de minister dat de politie niet rechtstreeks in kennis wordt gesteld. Het parket wordt gecontacteerd om de kwestie in detail te bespreken, zodat de informatie op het juiste moment wordt bezorgd. De strafuitsluitingsgronden behoren trouwens tot de bevoegdheid van het parket.

De minister van Defensie verduidelijkt dat het PNR-arrest enkele dagen geleden werd gewezen, dat het op dit moment wordt bestudeerd en dat de wetgeving indien nodig nog zal worden aangepast.

IV. — **ARTIKELSGEWIJZE BESPREKING EN STEMMINGEN**

Artikel 1

Dit artikel bevat de grondwettelijke bevoegdheidsgrondslag.

Artikel 1 wordt eenparig aangenomen.

Art. 2

Er worden over dit artikel geen opmerkingen gemaakt.

Artikel 2 wordt eenparig aangenomen.

Art. 3

Dit artikel beoogt de wijziging van artikel 11 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

Mevrouw Sophie De Wit (N-VA) stelt vast dat dit artikel de wettelijke basis vormt opdat de ADIV zich bij een nationale cybersecuritycrisis ten dienste van de natie kan stellen. De memorie van toelichting bevat evenwel nauwelijks argumentatie waarom deze taak aan de ADIV wordt toegewezen. Dit is, zoals ook het advies van het

pas aisé pour le SGRS de l'assurer, comme l'indique également l'avis du Comité permanent R. La membre demande dès lors si le SGRS dispose des moyens humains et financiers nécessaires pour prendre en charge cette mission additionnelle.

L'intervenante poursuit en soulignant que le Conseil d'État indique à propos du volet "Menace des intérêts vitaux du pays ou des besoins essentiels de la population" que l'exposé des motifs renvoie à une définition qui 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". Le Conseil d'État a recommandé de faire figurer cette définition dans la loi, mais aucune suite n'a été donnée à cette recommandation. La ministre pourrait-elle fournir des explications à ce propos?

En outre, le Comité permanent R souligne que la notion d'entités à protéger, c'est-à-dire les intérêts vitaux du pays ou les besoins essentiels de la population, est définie de manière trop large, et il propose d'utiliser la notion d'"infrastructures critiques", que la ministre estime trop restreinte. La membre estime toutefois que la notion de "besoins essentiels" est une notion fourre-tout.

Par ailleurs, le projet de loi à l'examen habilite non seulement le SGRS à neutraliser toute cyberattaque, mais l'autorise également à y réagir en menant lui-même une cyber contre-attaque. L'intervenante, tout comme le Comité permanent R, ignore toutefois quel est le cadre légal applicable. Il est renvoyé à 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 à 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. Or, la lecture de ces deux textes ne permet pas de comprendre pourquoi ceux-ci serviront de base légale aux cyber contre-attaques lancées par le SGRS. L'intervenante comprend que le SGRS espère secrètement qu'il sera soumis aux moins de restrictions possible pour pouvoir mener ses opérations en toute discrétion, dès lors qu'il est effectivement souvent préférable, dans ce type d'opérations, de pouvoir agir sans trop de bruit ni d'ingérence. Jusqu'à ce qu'évidemment les choses dérapent et que ce dérapage entraîne une escalade dont il convient d'assumer les répercussions et la responsabilité politique.

La ministre de la Défense aborde les conditions fixées pour déclencher une contre-attaque cyber. À ce sujet, elle indique tout d'abord qu'avec cet ajout, il n'est pas prévu d'installer un automatisme par lequel le SGRS réagirait à toute cyberattaque qui surviendrait sur des

Vast Comité I aangeeft, immers geen vanzelfsprekende taak voor de ADIV. Het lid wenst dan ook te vernemen of de ADIV wel over de nodige mensen en middelen beschikt om deze bijkomende taak op zich te nemen.

Zij merkt voorts op dat de Raad van State in zijn advies voor het onderdeel "de vitale belangen van het land of de essentiële behoeften van de bevolking bedreigt" aanstipt dat in de memorie van toelichting wordt verwezen naar een definitie die gebaseerd is die welke vervat is in artikel 2, § 2, van het koninklijk besluit van 18 april 1988 tot oprichting van het Coördinatie- en Crisiscentrum van de regering. De Raad van State acht het aangewezen deze definitie in de wet op te nemen, doch er werd hieraan geen gehoor gegeven. Kan de minister dit duiden?

Bovendien merkt het Vast Comité I op dat de te beschermen entiteiten, zijnde de vitale belangen van het land of de essentiële behoeften van de bevolking, een te ruime omschrijving is en stelt voor de woorden "kritieke infrastructuren" te gebruiken, wat volgens de minister dan weer te beperkend is. De notie "de essentiële behoeften" is volgens het lid evenwel dan weer een containerbegrip.

De ADIV krijgt voorts niet enkel de bevoegdheid om een cyberaanval te neutraliseren, maar kan ook reageren met een eigen cyberaanval. Het is de spreekster, net als het Vast Comité I, echter onduidelijk wat het wettelijk kader hiervoor is. Er wordt verwezen naar 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 naar het koninklijk besluit 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. Lezing ervan brengt evenwel geen duidelijkheid waarom dit als wettelijke basis dient voor een tegenaanval van de ADIV. De spreekster begrijpt dat zeker de ADIV onderhuids hoopt op zo min mogelijk begrenzingen om in stilte zijn ding te kunnen doen, en voor zulke aangelegenheden is het inderdaad vaak beter als er flexibel kan worden opgetreden zonder te veel ruchtbaarheid en inmenging. Tot het uiteraard eens verkeerd loopt met een escalatie waarvan de repercussies en de politieke verantwoordelijkheid moeten worden gedragen.

De minister van Defensie gaat in op de voorwaarden voor een cybertegenaanval. Ze wijst er allereerst op dat die toevoeging niet betekent dat de ADIV automatisch zal reageren op elke cyberaanval op niet-militaire Belgische systemen. Daarvoor is elke cyberaanval op zich te

systèmes belges non militaires. La réalité de chaque cyberattaque individuelle est trop complexe pour cela, et en même temps, la réponse opérationnelle la plus appropriée doit être envisagée. L'objectif de cet ajout est plutôt de créer un cadre juridique qui permettrait au SGRS d'éventuellement répondre à une cyberattaque sur des systèmes belges non militaires, en cas de nécessité.

Deuxièmement, la ministre insiste sur le fait qu'il s'agit d'une contre-attaque cyber, en réaction à une attaque contre des systèmes belges. Cela implique que le SGRS peut lancer une contre-attaque cyber directement contre l'auteur de l'attaque initiale, dans l'objectif d'arrêter l'attaque en soi. L'objectif n'est pas que le SGRS réagisse excessivement sur une attaque, mais bien d'arrêter l'attaque cyber.

Le SGRS doit être sollicité pour répondre par une attaque en cas de "crise nationale cyber". La notion de "crise nationale cyber" vient du Plan d'urgence cyber qui a été approuvé par le gouvernement belge en 2017. Ce Plan décrit à partir de quel moment il est question d'une "crise nationale cyber". Ce sont le *Centre for Cyber Security Belgium* (CCB) et le Centre de Crise National (NCCN) qui déclenchent la crise nationale et qui sont chargés de réunir tous les acteurs gouvernementaux concernés, dont le SGRS et la Défense. Cette "crise nationale cyber", gérée en concertation avec les autres services de sécurité belges, est donc une condition *sine qua non* pour que soit lancée une contre-attaque. Il faut par ailleurs prendre en compte le côté technique d'une attaque, autrement dit, le type d'attaque qui se présente. De nombreux facteurs entrent en jeu pour juger de la nécessité et de la nature de la contre-attaque.

Quant au cadre juridique, la disposition précise bien que la réplique du SGRS doit respecter le droit international. Ce terme vise non seulement les règles qui s'appliquent pour déterminer si une attaque est légale – par exemple, la Charte de l'ONU qui reconnaît aux États le droit à la légitime défense – mais aussi le droit international humanitaire et le droit des conflits armés, qui précise les règles à suivre dans la conduite des hostilités. La contre-attaque cyber peut aussi être une réaction à une violation moins grave du droit international; par exemple, une cyber-attaque visant à altérer les résultats d'une élection serait une violation de la souveraineté belge. Pour arrêter cette attaque, le SGRS pourrait être amené à lancer une contre-attaque pour faire cesser cette violation.

La contre-attaque cyber doit aussi répondre à l'ensemble des normes de droit international applicables aux cas d'espèce et les règles applicables peuvent varier en fonction des circonstances. La décision de riposter est complex, en tegelijk moet steeds worden nagedacht over hoe het best operationeel wordt gereageerd. Met die toevoeging wordt veeleer beoogd een wettelijk kader te creëren dat de ADIV in de mogelijkheid zou stellen indien nodig eventueel te reageren op een cyberaanval op niet-militaire Belgische systemen.

Ten tweede benadrukt de minister dat het een cybertegenaanval betreft, als reactie op een aanval op Belgische systemen. Zulks betekent dat de ADIV een rechtstreekse cybertegenaanval kan uitvoeren tegen de dader van de initiële aanval, om de eigenlijke aanval te stoppen. Het is niet de bedoeling dat de ADIV buitensporig reageert op de aanval, maar wel de cyberaanval te doen stoppen.

Bij een "nationale cybercrisis" moet de hulp van de ADIV worden ingeroepen om in de tegenaanval te gaan. Het concept "nationale cybercrisis" komt uit het door de Belgische regering in 2017 goedgekeurde cybernoodplan, waarin wordt beschreven vanaf wanneer sprake is van een "nationale cybercrisis". Het Centrum voor Cybersecurity België (CCB) en het Nationaal Crisiscentrum (NCCN) roepen de nationale crisis uit en moeten alle betrokken overheidsactoren samenroepen, waaronder de ADIV en Defensie. Die "nationale cybercrisis" wordt beheerd in overleg met de andere Belgische veiligheidsdiensten en vormt dan ook een *conditio sine qua non* om een tegenaanval uit te voeren. Voorts moet rekening worden gehouden met de technische kant van een aanval, dus met het soort van aanval. Heel wat factoren zullen bepalen of een tegenaanval vereist is en waaruit die moet bestaan.

Wat het wettelijk kader betreft, verduidelijkt de bepaling dat de reactie van de ADIV in overeenstemming moet zijn met het internationaal recht. Daarmee worden niet louter de geldende regels beoogd om te bepalen of een aanval wettelijk is – zo erkent het VN-Handvest het recht op zelfverdediging van de Staten –, maar ook het internationaal humanitair recht en het recht van de gewapende conflicten, dat bepaalt welke regels van toepassing zijn bij het verloop van vijandelijkheden. De cybertegenaanval kan ook een reactie zijn op een minder ernstige schending van het internationaal recht; een cyberaanval die wordt uitgevoerd om de uitslag van een verkiezing te wijzigen, zou bijvoorbeeld een schending van de Belgische soevereiniteit vormen. Om die aanval te stoppen en die schending een halt toe te roepen, zou de ADIV een tegenaanval kunnen uitvoeren.

De cybertegenaanval moet tevens voldoen aan alle in dezen toepasselijke normen van internationaal recht, en de geldende regels kunnen verschillen naargelang van de omstandigheden. De beslissing om te reageren houdt

une mise en œuvre des forces armées. C'est la ministre ou le gouvernement, en fonction des circonstances, qui peuvent prendre cette décision sur la base de l'arrêté royal du 6 juillet 1994.

À la question de savoir s'il y a du personnel en suffisance, la ministre explique que depuis sa prise de fonctions, elle s'attelle à renforcer la défense, y compris le SGRS. Des moyens complémentaires ont été libérés et plusieurs dizaines de personnes ont été engagées et le seront encore tout au long de l'année pour renforcer les services du SGRS. La ministre reconnaît que le SGRS a connu des crises par manque de personnel mais assure qu'une concertation a été menée avec les responsables du SGRS pour définir précisément quels sont les besoins et les priorités et dresser sur cette base un plan d'action. Des moyens conséquents ont maintenant été libérés et un recrutement massif a été lancé, notamment pour activer une cinquième composante cyber au sein de la défense d'ici la fin de la législature.

En ce qui concerne la suggestion du Comité permanent R de remplacer la notion d'"intérêts vitaux" par celle d'"infrastructure critique", la ministre précise que les critères repris dans ce projet de loi proviennent du Plan national d'urgence Cyber qui a été approuvé en 2017 par le gouvernement de l'époque. Les critères du plan d'urgence cyber sont quant à eux directement issus de l'arrêté royal du 18 avril 1988, portant création du Centre gouvernemental de coordination et de crise. En d'autres termes, ces critères sont utilisés depuis des décennies pour déterminer s'il est question d'une crise nationale, en l'occurrence dans le domaine cyber. Changer les critères signifierait ne plus être en conformité avec les dispositions de l'arrêté royal de 1988 et du Plan d'urgence de 2017, autrement dit, s'écarter des concepts qui ont été utilisés par les services pendant longtemps et sont compris de la même manière. L'objectif est également de faire une distinction avec les "incidents" de cybersécurité du plan d'urgence cyber, qui ne remplissent pas les conditions cumulées d'une "crise nationale". Le but n'est en effet pas que le SGRS soit compétent pour tout incident mais uniquement s'il s'agit d'une crise nationale nécessitant une telle coordination.

À la question de savoir pourquoi une nouvelle compétence a été ajoutée, la ministre répond que la menace cyber prend de plus en plus d'ampleur, comme l'ont montré les attaques contre le SPF Intérieur et le ministère de la Défense l'année dernière. Les cyberattaques sont particulièrement étendues et sont capables de paralyser des organisations entières, voire des pays. La Belgique a donc le devoir de protéger sa population et sa société contre cette menace. Ces dernières

in dat de strijdkrachten worden ingezet. Naargelang van de omstandigheden komt het de minister of de regering toe die beslissing te nemen, op grond van het koninklijk besluit van 6 juli 1994.

Op de vraag of er genoeg personeel is, antwoordt de minister dat zij sinds haar aantreden ijvert voor meer middelen voor Defensie, ook voor de ADIV. Er werden extra middelen vrijgemaakt; er werden tientallen medewerkers aangeworven of zullen in de loop van het jaar in dienst worden genomen, om de ADIV te versterken. De minister erkent dat de ADIV door personeelsgebrek in crisis heeft verkeerd, maar verzekert dat werd overlegd met de ADIV-directie om te bepalen wat nu precies de noden en prioriteiten zijn, en om op basis daarvan een actieplan uit te werken. Thans werden aanzienlijke middelen vrijgemaakt en werden medewerkers op grote schaal geworven, onder meer om tegen het einde van de regeerperiode binnen Defensie van start te gaan met een vijfde component, gespecialiseerd in cyberveiligheid.

Met betrekking tot het voorstel van het Vast Comité I om het begrip "vitale belangen" te vervangen door "kritische infrastructuur", verduidelijkt de minister dat de in dit wetsontwerp opgenomen criteria zijn overgenomen uit het Nationaal Cybernoodplan dat in 2017 werd goedgekeurd door de toenmalige regering. De criteria van het cybernoodplan komen dan weer rechtstreeks uit het koninklijk besluit van 18 april 1988 tot oprichting van het Coördinatie- en Crisiscentrum van de regering. Die criteria worden dus al tientallen jaren gebruikt om te bepalen of sprake is van een nationale crisis, in dit geval op cybervlak. Indien de criteria zouden worden veranderd, zou een en ander niet langer in overeenstemming zijn met de bepalingen van het koninklijk besluit van 1988 en evenmin met die van het noodplan van 2017; men zou dus afwijken van concepten die sinds jaar en dag door de diensten worden gehanteerd en die op eenvormige wijze worden geïnterpreteerd. Voorts is het de bedoeling een onderscheid te maken met de in het cybernoodplan vermelde cyberveiligheidsincidenten die niet voldoen aan alle voorwaarden waaraan een "nationale crisis" moet voldoen. Het is immers niet de bedoeling dat de ADIV bevoegd zou zijn voor elk incident, maar wel louter dat die dienst bij een nationale crisis de beoogde vereiste coördinatie op zich zou nemen.

Op de vraag waarom een nieuwe bevoegdheid werd toegevoegd, antwoordt de minister dat de cyberdreiging almaar grootschaliger wordt, zoals blijkt uit de aanvallen die vorig jaar werden uitgevoerd tegen de FOD Binnenlandse Zaken en tegen het ministerie van Defensie. De cyberaanvallen zijn bijzonder uitgebreid en kunnen volledige organisaties en zelfs landen verlammen. Ons land heeft dus de plicht zijn bevolking en samenleving tegen die dreiging te beschermen. De

années, plusieurs initiatives ont été prises à cette fin, à commencer par la création du *Centre for Cyber Security Belgium* (CCB) et, plus récemment, avec l'approbation du Plan national d'urgence cybernétique en 2017 et de la Stratégie Cybersécurité 2.0 en 2021. De cette manière, la coordination et la circulation des informations entre les services de sécurité belges sont assurées en cas de cyberattaque. Le SGRS et la Défense y jouent un rôle majeur et ont expressément souhaité s'engager à utiliser leurs propres capacités à des fins autres que militaires.

Concernant la recommandation du Conseil d'État de reprendre dans la loi la définition d' "intérêts vitaux", la ministre explique que les "intérêts vitaux" ou les "besoins essentiels de la population" auxquels renvoie cette notion ont été définis dans l'exposé des motifs. Il s'agit de: 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; et l'intégrité du territoire national. La définition des intérêts vitaux est une notion susceptible d'évoluer rapidement, raison pour laquelle il a été jugé préférable de ne pas en reprendre la définition dans le projet de loi, pour ne pas devoir changer régulièrement le contenu de la loi par la suite. Mettre la définition dans l'exposé des motifs donne davantage de flexibilité aux services de renseignement pour répondre aux attentes vis-à-vis de ces "intérêts vitaux".

L'article 3 est adopté à l'unanimité.

Art. 4 et 5

Ces articles ne donnent lieu à aucune observation.

Les articles 4 et 5 sont successivement adoptés à l'unanimité.

Art. 6

Cet article modifie l'article 13/1 de la même loi.

Mme Sophie De Wit (N-VA) souligne que cet article concerne la commission d'infractions par les agents.

Le paragraphe 8 dispose que, si la commission BIM a émis une décision négative ou n'a pas pris de décision dans le délai légal, le Comité permanent R décidera

jongste jaren werden daartoe meerdere initiatieven genomen, zoals de oprichting van het *Center for Cyber Security Belgium* (CCB), en recenter ook de goedkeuring van het Nationaal Cybernoodplan in 2017 en van de Cybersecurity Strategie België 2.0 in 2021. Aldus is bij een cyberaanval de coördinatie en de informatiedoorstroming tussen de Belgische veiligheidsdiensten gewaarborgd. De ADIV en Defensie spelen daarin een grote rol en hebben uitdrukkelijk aangegeven dat zij zich ertoe willen verbinden hun eigen mogelijkheden ook voor niet-militaire doeleinden in te zetten.

Met betrekking tot de aanbeveling van de Raad van State om de definitie van het begrip "vitale belangen" in de wet op te nemen, geeft de minister aan dat in de memorie van toelichting wordt verduidelijkt wat met "vitale belangen of essentiële behoeften van de bevolking" wordt bedoeld. Het betreft de openbare orde (dus de openbare rust, de volksgezondheid en de openbare veiligheid), het wetenschappelijk en economisch potentieel van het land, de nationale soevereiniteit en de bij de Grondwet en de wetten opgerichte instellingen, alsook de integriteit van het nationaal grondgebied. "Vitale belangen" is een begrip dat snel kan evolueren; om die reden werd er de voorkeur aan gegeven de omschrijving niet in het wetsontwerp op te nemen, teneinde de inhoud van de wet achteraf niet om de haverklap te moeten wijzigen. De omschrijving ervan in de memorie van toelichting biedt het voordeel dat de veiligheidsdiensten meer flexibiliteit krijgen om tegemoet te komen aan de verwachtingen inzake die "vitale belangen".

Artikel 3 wordt eenparig aangenomen.

Art. 4 en 5

Er worden over deze artikelen geen opmerkingen gemaakt.

De artikelen 4 en 5 worden achtereenvolgens eenparig aangenomen.

Art. 6

Dit artikel beoogt artikel 13/1 van dezelfde wet te wijzigen.

Mevrouw Sophie De Wit (N-VA) stipt aan dat dit artikel betrekking heeft op het plegen van strafbare feiten door agenten.

Paragraaf 8 bepaalt dat als de BIM-commissie een negatieve beslissing of geen beslissing heeft uitgebracht binnen de wettelijke termijn, het Vast Comité I beslist

d'autoriser ou non l'infraction. La commission BIM n'est pas favorable à cette nouvelle compétence du Comité permanent R, à savoir la compétence de révoquer une décision de la commission BIM.

En ce qui concerne le paragraphe 10, qui a trait à l'arrêt de la mesure par le dirigeant du service, la commission BIM estime qu'elle doit pouvoir retirer à tout moment son autorisation de commettre des infractions si elle constate que la mesure n'est plus nécessaire pour le succès de la mission ou pour assurer la sécurité de l'agent ou de tiers, qu'elle n'est plus utile pour atteindre l'objectif visé, qu'elle ne satisfait plus à la condition de proportionnalité et qu'une illégalité est constatée. Selon le projet de loi, la commission BIM ne peut cependant retirer son accord qu'en cas d'illégalité et non si les autres conditions ne sont plus remplies. Pourquoi cette restriction de sa fonction de contrôle? La membre souligne également que le Comité permanent R lui-même est d'avis que le pouvoir de contrôle de la commission BIM devrait être plus large. La commission BIM elle-même plaide en faveur d'un pouvoir de contrôle complet.

La ministre de la Défense rappelle tout d'abord que les infractions doivent être directement proportionnelles à l'objectif visé par la mission et ne peuvent pas porter atteinte à l'intégrité physique des personnes. La commission d'infractions est soumise tant à un contrôle interne qu'à un contrôle externe. Le contrôle interne consiste en l'approbation de la demande par le chef de service et le contrôle externe consiste en l'approbation par la commission BIM qui décrit précisément les faits susceptibles d'être qualifiés d'infractions, le contexte de la demande, la finalité, la liste des agents répondant au profil requis pour commettre les faits et la proportionnalité. En cas d'approbation, le Comité permanent R est ensuite informé de l'opération et dispose d'un pouvoir de contrôle sur l'opération. Tant la commission BIM que le Comité permanent R ont accès, à tout moment, aux documents liés à l'opération et ont la possibilité d'y mettre fin dès qu'ils constatent une illégalité.

Mme Sophie De Wit (N-VA) répète que le paragraphe 10 prévoit clairement que la commission BIM et le Comité permanent R ne peuvent retirer leur accord qu'en cas d'illégalité.

Le ministre de la Justice renvoie, en l'occurrence, à l'exposé des motifs, qui indique ce qui suit: "En ce qui

of het strafbaar feit al dan niet wordt toegestaan. De BIM-commissie is geen voorstander van deze nieuwe bevoegdheid voor het Vast Comité I, namelijk de bevoegdheid om een beslissing van de BIM-commissie te herroepen.

Aangaande paragraaf 10, dat betrekking heeft op de beëindiging van de maatregel door het diensthoofd, is de BIM-commissie van oordeel dat zij haar akkoord om strafbare feiten te plegen op ieder moment moet kunnen intrekken wanneer zij vaststelt dat de maatregel niet meer noodzakelijk is voor het welslagen van de opdracht of ter verzekering van de veiligheid van de agent of die van derden, niet langer nuttig is voor het doel waarvoor het werd aangevraagd, niet meer voldoet aan de proportionaliteitsvereiste en bij vaststelling van een onwettigheid. Volgens het wetsontwerp kan de BIM-commissie haar akkoord evenwel slechts intrekken indien er sprake is van onwettigheid en niet indien de andere voorwaarden niet meer vervuld zijn. Vanwaar deze beperking op hun controlefunctie? Het lid vestigt er ook de aandacht op dat het Vast Comité I zelf van oordeel is dat de controlebevoegdheid van de BIM-commissie ruimer moet. De BIM-commissie zelf pleit voor een volledige controlebevoegdheid.

De minister van Defensie wijst er vooreerst op dat de strafbare feiten rechtstreeks in verhouding moeten staan tot de beoogde doelstelling van de opdracht en geen afbreuk mogen doen aan de fysieke integriteit van de betrokkenen. Het plegen van strafbare feiten is onderworpen aan zowel een interne als een externe controle. De interne controle komt neer op de goedkeuring van het verzoek door het diensthoofd, en de externe controle komt neer op de goedkeuring door de BIM-commissie waarin nauwkeurig wordt omschreven welke feiten als strafbaar kunnen worden gekwalificeerd, alsook wat de context en het doel van het verzoek is. Voorts bevat dat verzoek de lijst van de agenten die beantwoorden aan het vereiste profiel om de feiten te plegen en wordt de proportionaliteit van de feiten erin toegelicht. Indien het verzoek wordt goedgekeurd, wordt vervolgens het Vast Comité I van de operatie in kennis gesteld. Het beschikt vanaf dat moment over een controlebevoegdheid over de operatie. Zowel de BIM-commissie als het Vast Comité I hebben op elk moment toegang tot de documenten die verband houden met de operatie, die ze overigens mogen stopzetten zodra ze een onwettigheid vaststellen.

Mevrouw Sophie De Wit (N-VA) herhaalt dat paragraaf 10 duidelijk bepaalt dat de BIM-commissie en het Vast Comité I hun akkoord enkel kunnen intrekken indien er sprake is van onwettigheid.

De minister van Justitie verwijst in dezen naar de memorie van toelichting waarin het volgende wordt gesteld:

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." (DOC 55 2706/001, p. 30).

La ministre de la Défense explique que le contrôle de la légalité consiste à vérifier, de manière plus large, que les conditions légales sont respectées, par exemple que l'infraction est absolument nécessaire. Le contrôle se fait donc *a priori* et a posteriori, d'où la notion de double contrôle.

Mme Sophie De Wit (N-VA) comprend qu'il y ait un double contrôle, mais le deuxième contrôle se fait, pour ainsi dire, avec un bras attaché dans le dos. Le dirigeant du service applique différents critères, mais la commission BIM et le Comité permanent R peuvent retirer leur accord uniquement lorsqu'une illégalité est constatée et non sur la base de leur jugement concernant l'utilité, la nécessité ou la proportionnalité. Les deux instances auraient donc préféré qu'il en soit autrement. Elle souligne à cet égard que, conformément au paragraphe 11, les membres de la commission BIM ont accès aux données relatives à la mesure, peuvent se saisir de toutes les pièces utiles et entendre les membres du service et peuvent donc évaluer la situation.

Le ministre de la Justice souligne que la commission BIM n'effectue qu'un contrôle de légalité et ne procède pas à une évaluation de la situation telle qu'elle se présente sur le terrain. C'est le dirigeant du service qui s'en charge. En l'occurrence, chacun remplit un rôle et une tâche différents. Les compétences sont déterminées en conséquence.

La ministre de la Défense confirme que la commission BIM a accès à toutes les informations, de manière à pouvoir exercer un contrôle, mais elle souligne que c'est le chef de service qui juge de l'opportunité et qu'il peut interrompre l'opération en cours de route s'il juge qu'elle n'est plus opportune. Une distinction doit être faite entre l'opérationnalité et le rôle de contrôle de la commission BIM.

Mme Sophie De Wit (N-VA) prend acte du choix effectué et conclut que les avis du Comité permanent R et de la commission BIM ne sont pas suivis en l'occurrence.

L'article 6 est adopté par 9 voix et 3 abstentions.

"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." (DOC 55 2706/001, blz. 30).

De minister van Defensie legt uit dat de wettigheidscontrole inhoudt dat op zo ruim mogelijke wijze wordt nagegaan of de wettelijke voorwaarden, bijvoorbeeld dat het strafbaar feit absoluut noodzakelijk is, worden nageleefd. De controle gebeurt dus zowel *a priori* als *a posteriori*, vandaar dat men het heeft over een dubbele controle.

Mevrouw Sophie De Wit (N-VA) begrijpt dat er een dubbele controle is, maar de tweede controle gebeurt als het ware met een arm gebonden op de rug. Het diensthoofd hanteert verschillende criteria, doch de BIM-commissie en het Vast Comité I kunnen hun akkoord enkel intrekken bij de vaststelling van een onwettigheid en niet op basis van hun oordeel inzake de nuttigheid, de noodzakelijkheid dan wel de proportionaliteit. De beide instanties hadden dit dan ook graag anders gezien. Zij stipt in dit verband aan dat de leden van de BIM-commissie overeenkomstig paragraaf 11 toegang hebben tot de gegevens met betrekking tot de maatregel, zich alle nuttige stukken kunnen toe-eigenen en de leden van de dienst kunnen horen en derhalve de situatie kunnen inschatten.

De minister van Justitie stipt aan dat de BIM-commissie enkel een legaliteitscontrole uitvoert en geen appreciatie maakt van de situatie zoals ze zich voordoet op het terrein. Het is het diensthoofd dat dit laatste doet. Elkeen vervult in dezen dan ook een andere rol en een andere taak. De bevoegdheden zijn dienovereenkomstig bepaald.

De minister van Defensie bevestigt dat de BIM-commissie, teneinde toezicht te kunnen uitoefenen, toegang heeft tot alle informatie, maar ze benadrukt dat het het diensthoofd toekomt te oordelen of de maatregel gepast is en de aan de gang zijnde operatie te onderbreken indien hij van oordeel is dat die niet langer gepast is. Er moet een onderscheid worden gemaakt tussen de operationaliteit en de toezichthoudende rol van de BIM-commissie.

Mevrouw Sophie De Wit (N-VA) neemt akte van de gemaakte keuze en besluit dat de adviezen van het Vast Comité I en de BIM-commissie hier niet worden gevolgd.

Artikel 6 wordt aangenomen met 9 stemmen en 3 onthoudingen.

Art. 7

Cet article vise à insérer, dans la même loi, un article 13/1/1 dans la nouvelle sous-section 1 de cette loi, insérée par l'article 5.

Mme Sophie De Wit (N-VA) précise que cet article concerne la commission d'infractions par des sources humaines. Comme cela a déjà été mentionné lors de la discussion générale, il s'agit d'une mesure lourde de conséquences, car elle donne à des "citoyens ordinaires" la permission de commettre des infractions. Différents niveaux de contrôle sont prévus à cet égard.

La commission BIM, le Collège des procureurs généraux et le Comité permanent R se posent tout de même de sérieuses questions à ce sujet. En ce qui concerne la comparaison avec les infiltrants civils en droit pénal, il est exact que ceux-ci sont utilisés dans un but différent. Mais cela ne change rien au fait qu'il existe de grandes similitudes dans les faits, le mode d'exécution et l'impact sur la vie privée des personnes concernées. L'utilisation de sources humaines en prévoyant la possibilité qu'elles commettent des infractions a une portée au moins aussi grande que l'infiltration civile et doit donc être utilisée et contrôlée avec la même prudence extrême.

La commission BIM préconise donc d'en faire une méthode exceptionnelle plutôt qu'une méthode ordinaire. En effet, dans le cas d'une méthode exceptionnelle, on contrôle non seulement l'infraction, mais aussi la méthode elle-même (la nécessité, la proportionnalité, l'utilité). En effet, il ne faut pas perdre de vue qu'il s'agit en l'occurrence d'un citoyen ordinaire et non d'un agent.

Le Collège des procureurs généraux ajoute que cela crée en fait un déséquilibre entre les sources humaines contrôlées par les services de renseignement et de sécurité et les informateurs/infiltrants civils contrôlés par les autorités policières et judiciaires. Selon le Collège, la réglementation proposée menace de donner lieu, en pratique, à des applications créatives où la nouvelle réglementation relative aux services de renseignement et de sécurité serait utilisée dans des dossiers judiciaires. En effet, les mécanismes de contrôle et d'accompagnement pour les infiltrants civils sont beaucoup plus stricts que dans la réglementation proposée pour les sources humaines. En outre, un informateur ne peut jamais être habilité à commettre une infraction. Le Collège des procureurs généraux est d'avis que le fait d'avoir recours à des sources humaines autorisées à commettre des infractions doit être explicitement classifié comme une méthode spécifique ou exceptionnelle. Sinon, n'importe quelle source humaine peut être autorisée à commettre des infractions pour toute mission de renseignement

Art. 7

Dit artikel strekt tot invoeging in dezelfde wet van een artikel 13/1/1 in de nieuwe onderafdeling 1, ingevoegd bij artikel 5, van deze wet.

Mevrouw Sophie De Wit (N-VA) verduidelijkt dat dit artikel het plegen van strafbare feiten door menselijke bronnen betreft. Het gaat hier, zoals tijdens de algemene bespreking al aangekaart, over een zeer ingrijpende maatregel, want men geeft aan een "gewone burger" de toelating om strafbare feiten te plegen. Er is in dit verband in verschillende controleniveaus voorzien.

De BIM-commissie, het College van procureurs-generaal en het Vast Comité I stellen zich hierover toch ernstige vragen. Wat de vergelijking met de burgerinfiltratie uit het strafrecht betreft, klopt het dat die wordt ingezet voor een ander doeleinde. Maar dat neemt niet weg dat in de feiten, in de manier van uitvoering en de invloed op de privacy van de betrokken personen er wel grote gelijkenissen zijn. De inzet van menselijke bronnen en de mogelijkheid dat zij strafbare feiten kunnen plegen, is minstens even ingrijpend als de burgerinfiltratie en hoort dus ook met dezelfde grote voorzichtigheid te worden ingezet en gecontroleerd.

De BIM-commissie pleit er dan ook voor hiervan een uitzonderlijke methode te maken in plaats van een gewone methode. Bij een uitzonderlijke methode wordt immers niet alleen het strafbaar feit gecontroleerd maar ook de methode op zich (de noodzakelijkheid, de proportionaliteit, de nuttigheid). Men mag immers niet uit het oog verliezen dat het hier gaat over een gewone burger en niet over een agent.

Het College van procureurs-generaal voegt hieraan toe dat aldus eigenlijk een onevenwicht wordt gecreëerd tussen de menselijke bronnen die worden gecontroleerd door de inlichtingen- en veiligheidsdiensten en de informanten/burgerinfiltranten die worden gecontroleerd door de politionele en de gerechtelijke autoriteiten. De voorgestelde regeling dreigt volgens het College creatieve toepassingen in de praktijk te doen ontstaan waarbij van de nieuwe regeling voor de inlichtingen- en veiligheidsdiensten in gerechtelijke dossiers gebruik wordt gemaakt. De controle- en begeleidingsmechanismen voor burgerinfiltratie zijn immers een stuk strenger bij de burgerinfiltratie dan bij de voorgestelde regeling voor de menselijke bronnen. Bovendien kan een informant nooit worden gemachtigd om een misdrijf te plegen. Het College van procureurs-generaal is van oordeel dat het werken met bronnen die strafbare feiten mogen plegen uitdrukkelijk als specifieke of uitzonderlijke methode moet worden geclassificeerd. Doet men dat niet, dan kan iedere menselijke bron worden gemachtigd om misdrijven te

relevant du champ d'application de la loi du 30 novembre 1998. En tout cas, selon le Collège, l'autorisation de commettre des infractions pour des sources humaines ne devrait jamais être utilisée pour contourner les prescriptions légales spécifiques prévues par les dispositions concernées de la loi du 30 novembre 1998.

Mme De Wit déplore dès lors que ces préoccupations soient ignorées.

Le ministre de la Justice est d'avis que la comparaison effectuée entre une source humaine et un infiltrant civil ne s'applique pas en l'occurrence. En effet, un infiltrant civil opère dans le cadre d'une enquête pénale tandis que dans le cas d'une source humaine, il s'agit d'une enquête de renseignement. Ce sont deux situations différentes. Dans son arrêt n° 64 du 22 avril 2021 rendu à la suite d'une question préjudicielle du Comité permanent R, la Cour constitutionnelle a explicitement confirmé ce point de vue. Le Collège des procureurs généraux et les autres demandent donc de modifier la méthode actuelle des sources humaines qui est utilisée depuis des années déjà, avec des analyses de risques, des notes d'approche et des rapports d'information. Selon eux, toute source humaine devrait à l'avenir être soumise à l'approbation préalable de la commission BIM. Eu égard à ce point de vue, la question se pose dès lors de savoir si on aurait toujours mal agi ces dernières années. Selon le ministre, ce n'est pas le cas.

Si la source humaine commet une infraction, l'approbation préalable de la commission BIM est bien entendu nécessaire, comme le décrit explicitement l'article à l'examen. Des conditions particulières s'appliquent. En cas d'urgence concernant une source humaine, l'approbation préalable de la commission BIM est requise, ce qui n'est pas le cas pour un agent qui s'infiltre et commet une infraction. La police travaille également avec des sources humaines et, là aussi, il n'y a pas de contrôle préalable; elles ne peuvent évidemment pas commettre d'infraction.

Mme Sophie De Wit (N-VA) ne remet pas en cause le fait que les sources humaines telles que les informateurs sont utilisées depuis longtemps. En effet, il serait faux d'affirmer que les méthodes utilisées pendant toutes ces années étaient inadéquates, à ceci près que, jusqu'alors, cette source humaine n'était pas autorisée à commettre une infraction. Il y a toutefois une différence entre demander des informations et commettre une infraction. De plus, il s'agira d'une méthode ordinaire et non exceptionnelle, si bien que la commission BIM ne pourra évaluer que l'infraction en elle-même et non le reste de l'opération, ce que la membre, ainsi que certaines instances consultatives, regrettent profondément.

plegen voor iedere inlichtingenopdracht die valt onder het toepassingsgebied van de wet van 30 november 1998. In ieder geval zou het toelaten van strafbare feiten door menselijke bronnen volgens het College nooit mogen worden gebruikt om de bijzondere wettelijke vereisten te omzeilen die door de desbetreffende bepalingen van de wet van 30 november 1998 zijn bepaald.

Mevrouw De Wit betreurt dan ook dan aan deze bezorgdheden wordt voorbijgegaan.

De minister van Justitie is van oordeel dat de gemaakte vergelijking tussen een menselijke bron en een burgerinfiltrant hier niet opgaat. Bij een burgerinfiltrant gaat het immers om een strafonderzoek, terwijl het bij een menselijke bron om een inlichtingenonderzoek gaat. Dit zijn twee verschillende situaties. In zijn arrest nr. 64 van 22 april 2021 naar aanleiding van een prejudiciële vraag van het Vast Comité I heeft het Grondwettelijk Hof dit standpunt uitdrukkelijk bevestigd. Het College van procureurs-generaal en de anderen vragen aldus de bestaande methode van menselijke bronnen die al jaren wordt gehanteerd, met risicoanalyses, benaderingsnota's en infoverslagen, te veranderen. Elke menselijke bron dient volgens hen in de toekomst voorafgaandelijk aan de goedkeuring van de BIM-commissie te worden onderworpen. Gelet op dit standpunt rijst dan ook de vraag of de voorbije jaren dan steeds verkeerd werd gehandeld, geenszins volgens de minister.

Als de menselijke bron een strafbaar feit pleegt, is er uiteraard de noodzaak van een voorafgaande goedkeuring door de BIM-commissie, wat uitdrukkelijk wordt beschreven in het ter bespreking voorliggende artikel. Er gelden bijzondere voorwaarden. In geval van hoogdringendheid bij een menselijke bron is een voorafgaand akkoord van de BIM-commissie vereist, wat niet het geval is bij een agent die infiltreert en een strafbaar feit pleegt. Ook de politie werkt met menselijke bronnen en ook daar is er geen voorafgaande controle; zij mogen natuurlijk geen strafbare feiten plegen.

Mevrouw Sophie De Wit (N-VA) trekt niet in twijfel dat al lang met menselijke bronnen zoals informanten wordt gewerkt. Het is inderdaad niet zo dat al die jaren verkeerdelijk werd gehandeld, evenwel met die nuance dat die menselijke bron tot dan geen strafbaar feit mocht plegen. Er is evenwel een verschil tussen informatie opvragen en strafbare feiten plegen. Bovendien wordt dit een gewone methode en geen uitzonderlijke, waardoor de BIM-commissie enkel het strafbaar feit op zich kan beoordelen en niet de rest van de operatie. De BIM-commissie kan de hele operatie dus niet controleren, wat het lid, samen met enkele adviesverlenende instanties, ten zeerste betreurt.

Quant à la révocation de l'accord pour commettre des infractions, la commission BIM estime qu'elle devrait pouvoir le retirer à tout moment, alors que, là aussi, seul le critère de légalité est retenu. Il s'agit donc de la même discussion que pour l'article 6.

L'article 7 est adopté par 9 voix contre 3.

Art. 8 et 9

Ces articles ne donnent lieu à aucune observation.

Les articles 8 et 9 sont successivement adoptés à l'unanimité.

Art. 10

Cet article modifie l'article 13/2 de la même loi.

Mme Sophie De Wit (N-VA) indique que cet article concerne le faux nom, la fausse qualité, l'identité fictive et la qualité fictive et note qu'ici aussi, aucune compétence de contrôle n'est confiée à la commission BIM, alors que cela lui semblerait opportun. En outre, le mot "temporaire" est supprimé sans autre argumentation. Aucune durée maximale n'est prévue, mais le contraire de temporaire est permanent/définitif et telle ne peut être l'intention.

La ministre de la Défense explique que le mot "temporaire" est supprimé car c'est un concept imprécis qui n'apporte, selon elle, aucune plus-value à l'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. Elle estime qu'il va de soi qu'un agent ne garde pas son identité fictive à vie et que la notion de temporaire, par contre, s'accommode mal avec des missions de longue durée.

En ce qui concerne les pouvoirs de contrôle BIM, la ministre fait remarquer que ce sont des mesures qui ne peuvent être mises en œuvre de manière autonome que pour protéger la sécurité des agents et des tiers. Elles ne peuvent être employées de manière autonome pour la récolte de données. En d'autres termes, le Comité R et la commission BIM disposent de l'ensemble de leurs pouvoirs de contrôle sur les méthodes de recueil de

Wat de herroeping van het akkoord tot het plegen van strafbare feiten betreft, is de BIM-commissie van oordeel dat zij dat akkoord op elk ogenblik zou moeten kunnen intrekken, terwijl ook hier enkel het wettigheidscriterium in aanmerking wordt genomen. Het gaat hier dus over dezelfde discussie als bij artikel 6.

Artikel 7 wordt aangenomen met 9 tegen 3 stemmen.

Art. 8 en 9

Er worden over deze artikelen geen opmerkingen gemaakt.

De artikelen 8 en 9 worden achtereenvolgens eenparig aangenomen.

Art. 10

Dit artikel beoogt artikel 13/2 van dezelfde wet te wijzigen.

Mevrouw Sophie De Wit (N-VA) stipt aan dat dit artikel de valse naam, valse hoedanigheid, fictieve identiteit en fictieve hoedanigheid betreft en merkt op dat hier in geen controlebevoegdheid voor de BIM-commissie is voorzien, terwijl dit volgens haar wel aangewezen zou zijn. Bovendien wordt zonder bijbehorende argumentatie het woord "tijdelijk" opgeheven. Er is evenmin in een maximumduur voorzien, maar het tegenovergestelde van tijdelijk is blijvend/definitief, en dat kan toch ook niet de bedoeling zijn.

De minister van Defensie geeft aan dat het woord "tijdelijk" werd geschrapt omdat het een vaag begrip is dat volgens haar geen enkele meerwaarde toevoegt aan het artikel. Integendeel, in de praktijk leidt het meer tot verwarring dan dat het een nuttige verduidelijking verschaft. Het is trouwens best mogelijk dat gedurende een lange periode een fictieve identiteit wordt gebruikt, bijvoorbeeld in het kader van een online surveillance. Ze vindt het vanzelfsprekend dat een agent zijn fictieve identiteit niet zijn hele leven behoudt en dat de term "tijdelijk", daarentegen, niet goed te verenigen valt met langdurige opdrachten.

Wat de BIM-controlebevoegdheden betreft, merkt de minister op dat dit maatregelen zijn die alleen autonoom kunnen worden aangewend om de veiligheid van de agenten en van derden te beschermen. Zij mogen niet autonoom worden aangewend voor het verzamelen van gegevens. Het Vast Comité I en de BIM-commissie beschikken derhalve over al hun controlebevoegdheden inzake de methoden voor het verzamelen van gegevens,

données, y compris lorsqu'une mesure d'appui est employée dans ce cadre. De plus, le Comité R est notifié systématiquement en cas de création d'identités fictives et à chaque fois qu'une telle identité fictive est employée.

Mme Sophie De Wit (N-VA) peut comprendre qu'il faille éviter d'être trop rigide, mais pourquoi ne pas prévoir une règle permettant de déterminer une période maximale? Toute période limitée est en effet temporaire. En l'absence de limite, la mesure est permanente et éternelle. La membre insiste donc sur l'importance de chaque mot dans cette problématique.

La ministre de la Défense souligne que le fait que l'identité fictive soit temporaire ou pas n'a pas d'incidence sur le contrôle. Pour elle, l'existence d'un contrôle permanent et le bon sens font que la présence ou non du mot "temporaire" dans le texte ne change rien au fond et à l'objectif poursuivi.

Mme Sophie De Wit (N-VA) attire l'attention sur le fait que la commission BIM n'est pas non plus favorable à la suppression du mot "temporaire".

L'article 10 est adopté par 9 voix et 3 abstentions.

Art. 11 à 16

Ces articles ne donnent lieu à aucune observation.

Les articles 11 à 16 sont successivement adoptés à l'unanimité.

Art. 17

Cet article vise à insérer un article 16/6 dans le chapitre III, section 4, sous-section 1re, de la même loi.

Mme Sophie De Wit (N-VA) constate qu'aujourd'hui, la demande de données financières constitue une méthode exceptionnelle. Le projet de loi entend en faire une méthode ordinaire, au motif que cette mesure ne serait pas si intrusive.

Or les informations demandées vont au-delà des simples données d'identification; il s'agit de fournir des informations sur la capacité financière d'une personne. Elle comprend qu'il puisse être nécessaire d'obtenir ces informations mais estime qu'il est souhaitable d'en faire

ook wanneer in dit verband een ondersteuningsmaatregel wordt gebruikt. Bovendien wordt het Vast Comité I systematisch op de hoogte gebracht wanneer er een fictieve identiteit wordt gecreëerd en telkens wanneer een dergelijke fictieve identiteit wordt gebruikt.

Mevrouw Sophie De Wit (N-VA) begrijpt dat men niet te rigide wil zijn, maar waarom niet in een regel voorzien die toelaat een maximumduur te bepalen? Elke begrensde periode is immers tijdelijk. Wanneer niet wordt begrensd, is de maatregel blijvend en eeuwigdurend. Het lid benadrukt in deze problematiek dan ook het belang van elk woord.

De minister van Defensie beklemtoont dat het feit dat een fictieve identiteit al dan niet tijdelijk is, geen weerslag heeft op het toezicht. Zij meent dat het bestaan van een permanent toezicht en het gezond verstand ervoor zorgen dat het al dan niet vermelden van het woord "tijdelijk" in de tekst ten gronde niets verandert, ook niet aan het nagestreefde doel.

Mevrouw Sophie De Wit (N-VA) vestigt er de aandacht op dat de BIM-commissie ook geen voorstander is van de opheffing van het woord "tijdelijk".

Artikel 10 wordt aangenomen met 9 stemmen en 3 onthoudingen.

Art. 11 tot 16

Er worden over deze artikelen geen opmerkingen gemaakt.

De artikelen 11 tot 16 worden achtereenvolgens eenparig aangenomen.

Art. 17

Dit artikel strekt tot invoeging van een artikel 16/6 in hoofdstuk III, afdeling 4, onderafdeling 1, van dezelfde wet.

Mevrouw Sophie De Wit (N-VA) merkt op dat het opvragen van financiële gegevens thans een uitzonderlijke methode is. Het wetsontwerp wil dit veranderen naar een gewone methode omdat deze maatregel niet zo ingrijpend zou zijn.

De opgevraagde informatie gaat evenwel verder dan loutere identificatiegegevens; het gaat over het geven van informatie van de financiële draagkracht van een persoon. Zij begrijpt dat het nodig kan zijn om deze informatie te krijgen, doch acht het raadzaam er een

une méthode spécifique, qui permette un contrôle plus poussé que ce qui est actuellement proposé.

Le ministre de la Justice souligne qu'il s'agit uniquement de l'identification et, plus particulièrement, de la réponse aux questions suivantes: "La personne en question a-t-elle un compte et, dans l'affirmative, lequel?" et "À qui appartient ce numéro de compte?". Il s'agit d'une méthode ordinaire, et la demande est immédiatement transmise au Comité permanent R qui en contrôle la légalité.

Comme pour les données télécoms, selon la jurisprudence de la Cour européenne, l'identification n'est "pas sensible". Il n'y a aucun lien avec la capacité financière des individus. Si cette information apparaît nécessaire, une méthode exceptionnelle doit être utilisée.

Mme Sophie De Wit (N-VA) fait observer que l'on parle ici de produits et de services financiers et que, lors de la compilation de toutes ces données, un grand nombre d'informations sont collectées, au-delà de simples données d'identification. À cet égard, elle partage la préoccupation du Comité permanent R et de la commission BIM, qui indique dans son avis que l'argumentation de l'exposé des motifs ne pouvait être suivie car l'instantané des relations bancaires d'une personne (comptes bancaires, comptes d'épargne, comptes-titres, comptes de placement, ouvertures de crédit, prêts, assurances-vie, …) n'est pas comparable à l'instantané de ses moyens de communication électronique (numéros d'appel, numéros IMEI). Selon la commission BIM, cette méthode devrait plutôt être qualifiée de nouvelle méthode particulière plutôt que de nouvelle méthode ordinaire.

Le ministre de la Justice estime que tous les éléments doivent être situés dans leur contexte et donne l'exemple du Point de contact central des comptes et contrats financiers (PCC), qui peut être consulté par les instances ordinaires, les notaires et d'autres personnes, sans autorisation préalable de la commission BIM.

Il s'agit en l'espèce de menaces contre la sécurité nationale.

Il maintient par conséquent sa position.

Mme Sophie De Wit (N-VA) répond qu'elle ne voit aucun problème à ce que les données soient contrôlées et souligne que la demande visant à renforcer le contrôle de cette méthode émane de la commission BIM et du Comité permanent R, c'est-à-dire des instances qui traitent cette matière au quotidien.

specifieke methode van te maken, wat meer controle toelaat dan wat nu wordt voorgesteld.

De minister van Justitie benadrukt dat het hier enkel de identificatie betreft en in het bijzonder het antwoord op de vragen: "Heeft de persoon in kwestie een rekening, en zo ja welke?" en "Van wie is dit rekeningnummer?". Het is een gewone methode waarbij onmiddellijk de vraag wordt overgezonden aan het Vast Comité I dat de wettigheid controleert.

Net zoals bij telecomgegevens is volgens de rechtspraak van het Europees Hof de identificatie "niet gevoelig". Er is geen link naar de financiële draagkracht van personen. Als dat noodzakelijk wordt, moet er een uitzonderlijke methode worden aangewend.

Mevrouw Sophie De Wit (N-VA) merkt op dat het gaat over financiële producten en diensten en dat bij het samenleggen van al die gegevens heel wat informatie wordt verzameld, meer dan alleen maar identificatiegegevens. Zij deelt in dezen dan ook de bezorgdheid van het Vast Comité I en van de BIM-commissie, die in haar advies heeft gesteld dat de argumentatie uit de memorie van toelichting niet kan worden gevolgd omdat de foto van iemands bankrelaties (bank-, spaar-, effecten- en beleggingsrekeningen, kredietopeningen, leningen, levensverzekeringen enzovoort) niet vergelijkbaar is met de foto van iemands elektronische communicatiemiddelen (oproepnummers, IMEI-nummers). Deze methode zou volgens de BIM-commissie beter worden gekwalificeerd als een nieuwe specifieke methode in plaats van als een nieuwe gewone methode.

De minister van Justitie meent dat alles in het juiste perspectief moet worden bekeken en geeft het voorbeeld van het Centraal Aanspreekpunt van rekeningen en financiële contracten (CAP) dat door gewone instanties, notarissen en andere kan worden geconsulteerd, zonder voorafgaande toestemming van de BIM-commissie.

In dezen gaat het over dreigingen tegen de nationale veiligheid.

Hij houdt dan ook vast aan zijn standpunt.

Mevrouw Sophie De Wit (N-VA) repliceert dat zij er geen problemen mee heeft dat de gegevens worden gecontroleerd en wijst erop dat de vraag om dienaangaande in een meer gecontroleerde methode te voorzien, komt van de BIM-commissie en het Vast Comité I, zijnde de instanties die hiermee dagelijks te maken hebben.

Le ministre de la Justice doute en outre que le schéma de vie d'un citoyen puisse être établi sur la base de quelques comptes.

Mme Sophie De Wit (N-VA) répond que le Comité permanent R indique ce qui suit dans son avis: "Le Comité Recommande de considérer cette méthode comme une méthode spécifique. Dans l'exposé des motifs, Ie gouvernement justifie le choix d'une méthode ordinaire en affirmant que "le caractère intrusif d'une telle méthode est (…) faible à très faible". Le Comité ne partage pas cet avis. Il est certain que lorsqu'un lien est établi entre la personne visée et certains produits et services financiers, des informations sont déjà communiquées sur la capacité financière de la personne concernée. Cela va donc au-delà des simples données d'identification.".

Il convient de préciser que ce problème est dénoncé par les "chiens de garde" eux-mêmes. Il est dès lors important pour le rapport que les ministres justifient les choix qu'ils ont faits.

L'article 17 est adopté par 9 voix et 3 abstentions.

Art. 18 à 25

Ces articles ne donnent lieu à aucune observation

Les articles 18 à 25 sont successivement adoptés à l'unanimité.

Art. 26

Cet article ne donne lieu à aucune observation.

L'article 26 est adopté par 9 voix et 3 abstentions

Art. 27

Cet article ne donne lieu à aucune observation.

L'article 27 est adopté à l'unanimité.

Des corrections d'ordre logistique sont apportées.

L'ensemble du projet de loi, tel qu'il a été corrigé sur le plan légistique, est adopté par vote nominatif par 9 voix et 3 abstentions.

De minister van Justitie betwijfelt ook of aan de hand van enkele rekeningen het levenspatroon van een burger kan worden bepaald.

Mevrouw Sophie De Wit (N-VA) antwoordt dat het Vast Comité I in zijn advies hierover het volgende stelt: "Het Comité beveelt aan om deze methode te kwalificeren als een specifieke methode. In de memorie van toelichting verantwoordt de regering de keuze voor een gewone methode door te stellen dat 'de intrusiviteit van een dergelijke methode (…) gering tot zeer gering is'. Het Comité is het hiermee niet eens. Zeker wanneer er een verband gelegd wordt tussen de geviseerde persoon en bepaalde financiële producten en diensten, wordt er reeds informatie meegedeeld over de financiële draagkracht van betrokkene. Dit gaat dus verder dan loutere identificatiegegevens.".

Het moge duidelijk zijn dat de waakhonden zelf dit aankaarten. Het is dan ook belangrijk voor het verslag dat de ministers de gemaakte keuzes met redenen omkleden.

Artikel 17 wordt aangenomen met 9 stemmen en 3 onthoudingen.

Art. 18 tot 25

Er worden over deze artikelen geen opmerkingen gemaakt.

De artikelen 18 tot 25 worden achtereenvolgens eenparig aangenomen.

Art. 26

Er worden over dit artikel geen opmerkingen gemaakt.

Artikel 26 wordt aangenomen met 9 stemmen en 3 onthoudingen.

Art. 27

Er worden over dit artikel geen opmerkingen gemaakt.

Artikel 27 wordt eenparig aangenomen.

Er worden wetgevingstechnische verbeteringen aangebracht.

Het gehele wetgevingstechnisch verbeterde wetsontwerp wordt bij naamstemming aangenomen met 9 stemmen en 3 onthoudingen.

Le résultat du vote nominatif est le suivant:

Ont voté pour:

Ecolo-Groen: Olivier Vajda, Stefaan Van Hecke;

PS: Khalil Aouasti, Laurence Zanchetta;

MR: Philippe Goffin, Philippe Pivin;

CD&V: Koen Geens;

Open Vld: Katja Gabriëls;

Vooruit: Ben Segers.

Ont voté contre: nihil

Se sont abstenus:

N-VA: Christoph D'Haese, Sophie De Wit, Kristien Van Vaerenbergh

Le rapporteur, *La présidente,*

Koen GEENS Kristien VAN VAERENBERGH

Articles nécessitant une mesure d'exécution (article 78.2, alinéa 4, du Règlement): *nihil*.

De naamstemming is als volgt:

Hebben voorgestemd:

Ecolo-Groen: Olivier Vajda, Stefaan Van Hecke;

PS: Khalil Aouasti, Laurence Zanchetta;

MR: Philippe Goffin, Philippe Pivin;

CD&V: Koen Geens;

Open Vld: Katja Gabriëls;

Vooruit: Ben Segers.

Hebben tegengestemd: nihil

Hebben zich onthouden:

N-VA: Christoph D'Haese, Sophie De Wit, Kristien Van Vaerenbergh.

De rapporteur, *De voorzitster,*

Koen GEENS Kristien VAN VAERENBERGH

Artikelen die een uitvoeringsmaatregel vereisen (artikel 78.2, vierde lid, van het Reglement): *nihil*

Imprimerie centrale – Centrale drukkerij