



ADVIES 002/VCI/2025 VAN 11 SEPTEMBER 2025

**INTERCEPTIES VAN BUITENLANDSE
COMMUNICATIE DOOR DE ADVI:
MEDEWERKINGSPLICHT TELECOMSECTOR
EN Vernietigingsprocedure onwettig
VERKREGEN GEGEVENS**

Gelet op het schrijven d.d. 28 juli 2025 van de minister van Defensie waarbij aan het Vast Comité I een advies gevraagd wordt over een ontwerp van koninklijk besluit houdende de regels voor de vernietiging van onwettig verkregen gegevens als bedoeld in artikel 44/4 van de Inlichtingenwet en houdende de regels voor samenwerking als bedoeld in artikel 44/5 van de Inlichtingenwet (hierna: Ontwerp).

Bevoegdheid Vast Comité I

Gelet op de artikelen 73 en 95 van de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

ADVIES

Context

Het Comité brengt in herinnering dat de betrokken regeling kadert binnen de implementatie van artikel 44 van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (Inlichtingenwet of WIV). Deze stelt:

“De Algemene Dienst Inlichting en Veiligheid kan elke vorm van communicatie uitgezonden of ontvangen in het buitenland opsporen, onderscheppen, afluisteren en er kennis van nemen alsook opnemen, volgens de nadere regels bepaald in de artikelen 44/3 en 44/4, in het kader van de opdrachten bedoeld in artikel 11, § 1, 1° tot 3° en 5°.”.

AVIS 002/CPR/2025 DU 11 SEPTEMBRE 2025

**INTERCEPTION DE COMMUNICATIONS À
L'ÉTRANGER PAR LE SGRS : CONCOURS DU
SECTEUR DES TÉLÉCOMMUNICATIONS ET
PROCÉDURE DE DESTRUCTION DES DONNÉES
ILLÉGALEMENT RECUEILLIES**

Vu le courrier du 28 juillet 2025 du ministre de la Défense demandant au Comité permanent R un avis sur un projet d'arrêté royal fixant les règles de destruction des données illégalement recueillies visées à l'article 44/4 de la Loi Renseignement et fixant les règles de coopération visées à l'article 44/5 de la Loi Renseignement (ci-après : le Projet).

Compétence du Comité permanent R

Vu les articles 73 et 95 de la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

AVIS

Contexte

Le Comité rappelle que la réglementation concernée s'inscrit dans le cadre de la mise en œuvre de l'article 44 de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (Loi Renseignement ou L.R&S). Celle-ci stipule que :

« Le Service Général du Renseignement et de la Sécurité peut rechercher, capter, écouter, prendre connaissance et enregistrer toute forme de communications émises ou reçues à l'étranger, selon les modalités fixées aux articles 44/3 et 44/4, dans le cadre des missions visées à l'article 11, § 1er, 1° à 3° et 5°. ».

Vernietiging van onwettig verkregen gegevens

1. Artikel 3 van het Ontwerp stelt dat “[d]e vernietiging van de onwettig verkregen gegevens [...] onder toezicht [gebeurt] van het diensthoofd of de daartoe door hem aangewezen persoon en in aanwezigheid van de functionaris van de gegevensbescherming van de ADIV”. Het Comité juicht de rol van de **functionaris van de gegevensbescherming (DPO)** in de voorgestelde regeling onverkort toe. Het is een duidelijke keuze van de minister van Defensie en de ADIV om de DPO een centrale rol toe te bedelen binnen de compliance van de inlichtingendienst.¹

2. Om een gedegen controle te kunnen verrichten op de uitvoering van de beslissing van het Comité tot vernietiging van de onwettig bevonden gegevens, is het Comité van oordeel dat in het Ontwerp moet worden toegevoegd dat de ADIV verplicht wordt om het **proces-verbaal van vernietiging** binnen de twee weken aan het Comité over te maken.

Medewerking van dienstenverstrekkers of netwerkoperatoren

3. De memorie van toelichting bij artikel 44 WIV stelt:

“Dit artikel 44 [...] begrenst de technische middelen niet waarop de ADIV een beroep mag doen om dergelijke intercepties uit te voeren. Dit artikel biedt dus het voordeel dat het de ADIV in de gelegenheid stelt niet beperkt te zijn tot het af luisteren van telefonie, maar zich aan te passen aan de nieuwe communicatietechnologieën die wereldwijd steeds veelvuldiger worden gebruikt (cf. het ITU-rapport – Internationale Telecommunicatie-Unie – 2014, dat gewag maakt van 3 miljard

Destruction des données illégalement recueillies

1. L'article 3 du Projet stipule que « [l]a destruction des données illégalement recueillies est réalisée sous le contrôle du dirigeant du service ou de la personne qu'il désigne à cet effet et en présence du délégué à la protection des données du SGRS ». Le Comité salue sans réserve le rôle du **délégué à la protection des données (DPO)** dans la réglementation proposée. Le ministre de la Défense et le SGRS ont clairement choisi de confier au DPO un rôle central dans le respect de la conformité (*compliance*) des services de renseignement.⁷

2. Afin de pouvoir contrôler de manière approfondie l'exécution de la décision du Comité de destruction des données jugées illégales, le Comité considère qu'il y a lieu d'ajouter dans le Projet que le SGRS est tenu de transmettre le **procès-verbal de destruction** au Comité dans un délai de deux semaines.

Coopération des fournisseurs de services ou des opérateurs du réseau

3. L'exposé des motifs à l'article 44 L.R.&S dispose que :

« Cet article 44 (ancien 259bis) ne délimite pas les moyens techniques auxquels le SGRS peut recourir pour procéder à de telles interceptions. Cet article a donc l'avantage de permettre au SGRS de ne pas rester cantonné aux écoutes en phonie mais de s'adapter aux nouvelles technologies de communication de plus en plus utilisées dans le monde (cf. le rapport UIT – Union Internationale des Télécommunications – 2014, qui fait état de 3 milliards d'individus utilisant l'internet), y

¹ Het Comité stelt vast dat deze rol van de DPO vooralsnog niet werd ingevoerd binnen de procedure tot vernietiging van onwettig door een BIM-methode verkregen gegevens (art. 13 KB 12 oktober 2010 houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten). Het Comité is van oordeel van deze bepaling zou dienen aangepast te worden aan de in voorliggend Ontwerp voorgestelde regeling.

⁷ Le Comité constate que ce rôle du DPO n'a pas encore été introduit dans la procédure de destruction des données illégalement recueillies par une méthode BIM (art. 13 de l'A.R. du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité). Le Comité estime que cette disposition devrait être adaptée à la réglementation proposée dans le présent Projet.

individuen die het internet gebruiken), ook door de terroristen, rebellen en andere aanverwante organisaties.

Gezien het feit dat steeds meer communicaties via kabels verlopen, met inbegrip van glasvezels, kan de ADIV niet anders dan nieuwe interceptiemethoden te ontwikkelen die hetgeen doorgaans "cable tapping" wordt genoemd, mogelijk maken. De ADIV kan zich immers niet veroorloven de talloze communicaties die op de kabels circuleren niet te kunnen intercepteren en, bij diezelfde gelegenheid, uitwisselingen tussen terroristische cellen of tussen rebellenfacties te missen.

De doelmatigste en snelste manier om aan cable tapping te doen, bestaat erin een beroep te doen op de medewerking van de netwerkoperatoren en verstrekkers van telecommunicatiediensten. De medewerking van bepaalde actoren die actief zijn in België, welke transmissiediensten via kabel naar en van het buitenland aanbieden, zou het immers eenvoudiger maken om communicatie- en gegevensstromen uitgezonden in het buitenland te intercepteren. Deze stromen zullen door de ADIV gefilterd worden op basis van het af luisterplan, teneinde daaruit enkel de in het buitenland uitgezonden communicaties en gegevens te halen, welke door dit plan en in verband met de opdrachten van de ADIV zijn toegestaan.

Het gaat dus altijd over gerichte intercepties. Geen enkele massacaptatie is wettelijk toegestaan."²

Krachtens artikel 44/3 WIV stelt de ADIV een lijst op "met organisaties of instellingen die het voorwerp zullen uitmaken van interceptie van hun communicaties" (het zgn. af luisterplan), die door de minister van Defensie dient te worden goedgekeurd. Deze lijsten "verantwoorden voor iedere organisatie of instelling de reden waarom zij het voorwerp is van een interceptie [...] in verband met de opdrachten bedoeld in artikel 11, § 1, 1° tot 3 en 5°, en vermelden de voorziene duur."

De memorie van toelichting verduidelijkt:
"Bovendien moet de interceptie gericht zijn op instellingen en organisaties die zich in het

compris par les terroristes, rebelles et autres organisations apparentées.

Eu égard au fait que de plus en plus de communications transitent via câbles, y compris les fibres optiques, le SGRS se doit de développer de nouveaux procédés d'interception permettant ce qu'on appelle communément le "cable tapping". En effet, le SGRS ne peut pas se permettre de ne pas pouvoir intercepter les nombreuses communications circulant sur les câbles et rater, par la même occasion, des échanges entre cellules terroristes ou entre factions rebelles.

La manière la plus efficiente et la plus rapide de faire du cable tapping est de solliciter la collaboration des opérateurs de réseau et des fournisseurs de services de télécommunications. La collaboration de certains opérateurs actifs en Belgique, qui offrent des services de transmission par câble vers et de l'étranger, permettrait en effet plus facilement d'intercepter des flux de communications et de données émises à l'étranger. Ces flux seront filtrés par le SGRS sur la base du plan d'écoute afin de n'extraire que les communications et données émises à l'étranger et autorisées par ce plan et en lien avec les missions du SGRS.

Il s'agira donc toujours bien d'interceptions ciblées. Aucune captation de masse n'est légalement autorisée."⁸

En vertu de l'article 44/3 L.R&S, le SGRS établit une liste « d'organisations et d'institutions qui feront l'objet d'interceptions de leurs communications » (ce que l'on appelle le plan d'écoute), que doit approuver le ministre de la Défense. Ces listes « justifieront pour chaque organisation ou institution la raison pour laquelle elle fera l'objet d'une interception, [...] en lien avec les missions visées à l'article 11, § 1er, 1° à 3° et 5°, et mentionneront la durée prévue. ».

L'exposé des motifs précise que :
« En outre, l'interception doit être ciblée sur des institutions et organisations se trouvant dans le

² Parl. St. Kamer 2015-2016, nr. 54-2043/001, 89.

⁸ Doc. parl. Chambre 2015-2016, n°54-2043/001, 89.

luisterplan bevinden [...]. Opnieuw, de regels tot intercepteren, filteren en het bepalen van doelwitten zijn al dertien jaar vastgelegd (door de wet van 3 april 2003). Het huidige voorstel vernieuwt niet. Er is vandaag evenmin sprake van massacaptatie als in 2003. Het feit dat interceptie doelgericht moet zijn en dus dat de stromen gefiltreerd moeten zijn, is in strijd met het principe van massacaptatie, in de zin dat het niet gaat over het opname van massale gegevens van het geheel van burgers, zonder enig discriminatie of gerechtvaardigd onderscheid. De captatie is gericht op organisaties of instellingen die een bedreiging vormen tegen de belangen die de ADIV dient te beschermen. De keuze van de doelwitten is gerechtvaardigd en gemotiveerd in een luisterplan dat wordt goedgekeurd door de minister van Landsverdediging en wordt doorgezonden aan het Comité I.³

En: "Er wordt daarnaast aan herinnerd dat de intercepties in functie van het af luisterplan en de opdrachten van de ADIV gericht zijn. Het spreekt vanzelf dat gezien de aard van de opdrachten van de ADIV in het buitenland dat de intercepties gebeuren met als objectief om de dreigingen tegen de troepen, de Belgische onderdanen, ... te identificeren. Het gaat dus eerst om een beperkt aantal organisaties waarvan het af luisteren relevant is in verhouding tot onderzochte doel die het voorwerp van de af luistering uitmaken en niet om voorafgaandelijk geïdentificeerde individuen. Gezien de gegevens gefilterd moeten worden, is het duidelijk dat de ADIV op geen enkel moment wettelijk kan overgaan tot een massale opname en vervolgens een massale exploitatie."⁴

Hieruit blijkt dat de ADIV niet bevoegd is om aan ongerichte massadatatapting te doen. Tegelijkertijd moet vermeld worden dat de wetgever de ADIV de mogelijkheid heeft gegeven om, binnen de grenzen van het af luisterplan dat gericht is op organisaties en instellingen, via betrokken methode aan *target discovery* te doen, zijnde het detecteren en

plan d'écoute, et ce en application de l'actuel article 44bis. A nouveau, les règles d'interception, de filtres et de cibles ont été fixées il y a treize ans (par la loi du 3 avril 2003). Le présent projet n'innove pas. Il n'est pas plus question de captation de masse aujourd'hui qu'en 2003. Le fait que l'interception doive être ciblée et donc que les flux doivent être filtrés s'oppose au principe de captation de masse, en ce sens qu'il ne s'agit pas de l'enregistrement d'une masse de données d'un ensemble de citoyens, sans aucune distinction ni discrimination justifiée. La captation est dirigée vers des organisations ou des institutions présentant une menace contre les intérêts à protéger par le SGRS. Le choix des cibles est justifié et motivé dans le plan d'écoute approuvé par le ministre de la Défense et transmis au Comité R. ».⁹

Et : « Par ailleurs, il est rappelé que les interceptions sont ciblées en fonction du plan d'écoute et des missions du SGRS. Il est évident qu'au vu de la nature des missions du SGRS à l'étranger, les interceptions se font avec l'objectif d'identifier les menaces contre les troupes, contre les ressortissants belges, ... Ce sont donc d'abord des organisations en nombre limité dont l'écoute est pertinente par rapport au but recherché qui font l'objet d'interceptions, et non des individus préalablement identifiés. Vu que les données doivent être filtrées, il est clair qu'à aucun moment, le SGRS ne pourrait légalement procéder à un enregistrement et ensuite une exploitation en masse. Les processus d'enregistrement et d'exploitation peuvent aisément être contrôlés par le Comité R. ».¹⁰

Il en ressort que le SGRS n'est pas habilité à procéder à une collecte massive et non ciblée de données. Il convient toutefois de mentionner que le législateur a donné au SGRS la possibilité, dans les limites du plan d'écoute visant les organisations et les institutions, de procéder à la *target discovery* (détection et identification des personnes physiques susceptibles de constituer

³ Parl. St. Kamer 2015-2016, nr. 54-2043/001, 91.

⁴ Parl. St. Kamer 2015-2016, nr. 54-2043/001, 83-84.

⁹ Doc. parl. Chambre 2015-2016, n° 54-2043/001, 91.

¹⁰ Doc. parl. Chambre 2015-2016, n° 54-2043/001, 83-84.

identificeren van fysieke personen die mogelijk een dreiging vormen.

Artikel 44/5 WIV stelt:

“Indien een ingreep op een communicatienetwerk noodzakelijk is om de interceptie van in het buitenland uitgezonden of ontvangen communicatie bedoeld in artikel 44 mogelijk te maken, wordt de operator van het netwerk of de verstrekker van de elektronische communicatiedienst met een schriftelijk verzoek van het diensthoofd aangezocht en is hij verplicht om zijn medewerking zo spoedig mogelijk te verlenen.

Eenieder die zijn medewerking weigert te verlenen aan de vorderingen bedoeld in het eerste lid, wordt gestraft met een geldboete van zesentwintig euro tot twintigduizend euro. De prestaties worden vergoed naargelang van de reële kosten, na voorlegging van de stavingstukken.

De Koning bepaalt, op voorstel van de Minister van Defensie en de Minister bevoegd voor de elektronische communicatie, de nadere regels voor deze medewerking.”.

Hoofdstuk 3 van voorliggend Ontwerp van KB regelt vernoemde samenwerking.

4. Artikel 14 van het Ontwerp stelt:

“De verstrekker van een elektronische communicatiedienst of de netwerkoperator zet een technisch systeem op dat automatische overdracht garandeert van stromen van gegevens en metagegevens van in het buitenland verzonden of ontvangen communicatie naar de apparatuur van de ADIV die is geplaatst bij de verstrekker van een elektronische communicatiedienst of de netwerkoperator.

De in het eerste lid vermelde apparatuur vervult de functie van technische filter om uitsluitend stromen van gegevens en metagegevens te onderscheppen van in geografische gebieden verzonden of ontvangen communicatie waar zich instellingen en organisaties bevinden die deel uitmaken van de lijsten als bedoeld in artikel 44/3 van de wet van 30 november 1998 en in het kader van de opdrachten bedoeld in artikel 11, §1, 1° tot 3° en 5° van voornoemde wet.”.

une menace) à l'aide de la méthode concernée.

L'article 44 L.R&S dispose que :

« Si une opération sur un réseau de communications est nécessaire pour permettre l'interception de communications émises ou reçues à l'étranger visée à l'article 44, l'opérateur du réseau ou le fournisseur du service de communications électroniques est saisi d'une demande écrite du dirigeant du service et est tenu de prêter son concours dans les plus brefs délais.

Toute personne qui refuse de prêter son concours aux réquisitions visées à l'alinéa 1er est punie d'une amende de vingt-six euros à vingt mille euros. Les prestations sont rétribuées selon les coûts réels, sur présentation des pièces justificatives.

Le Roi fixe, sur la proposition du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions, les modalités de ce concours. ».

Le chapitre 3 du présent Projet d'Arrêté royal règle ladite coopération.

4. L'article 14 du Projet prévoit que :

« Le fournisseur d'un service de communications électroniques ou l'opérateur du réseau met en place un système technique garantissant la transmission automatique des flux de données et de métadonnées de communications émises ou reçues à l'étranger vers les équipements du SGRS mis en place chez le fournisseur d'un service de communications électroniques ou l'opérateur du réseau.

Les équipements mentionnés à l'alinéa 1^{er} assurent la fonction de filtres techniques afin de n'intercepter que des flux de données et de métadonnées de communications émises ou reçues dans des zones géographiques où se trouvent des institutions et organisations qui font partie des listes visées à l'article 44/3 de la loi du 30 novembre 1998 et en lien avec les missions visées à l'article 11, § 1^{er}, 1° à 3° et 5° de ladite loi. ».

Het Comité brengt in herinnering, volgens de memorie van toelichting bij de wet van 30 maart 2017⁵, *“dat het voor de ADIV technisch mogelijk is om te bepalen of een communicatie zich al dan niet in het buitenland afspeelt.”*⁶

5. Het Comité stelt vast dat het Ontwerp het begrip **“automatische overdracht van stroom van gegevens en metagegevens”** introduceert. Dit wordt in art. 1, 10° omschreven als *“de geautomatiseerde verzending van stroom van gegevens en metagegevens, waarbij geen menselijke tussenkomst nodig is”*. Het Comité is van oordeel dat deze omschrijving niet afdoende is.

Vooreerst wordt in deze omschrijving het begrip **“metagegevens”** nergens verduidelijkt. Het Comité stelt zich de vraag of hiermee eenzelfde begrip bedoeld wordt als in art. 2, 93° van de Wet Elektronische Communicatie alwaar het begrip *“elektronische-communicatiemetagegevens”* wordt omschreven als *“de gegevens die worden verwerkt in een elektronische-communicatienetwerk met het oog op de transmissie, de distributie of de uitwisseling van de inhoud van elektronische communicatie, met inbegrip van gegevens waarmee een communicatie kan worden getraceerd en de bron en de bestemming van de communicatie kunnen worden bepaald, alsmede gegevens betreffende de locatie van de apparatuur die in het kader van het aanbieden van elektronische-communicatiediensten zijn gegenereerd, en de datum, het tijdstip, de duur en de aard van de communicatie”*. Noch in de aanhef van het Ontwerp noch in het bijhorende verslag aan de Koning wordt ter zake evenwel een link gelegd tussen het Ontwerp en de Wet Elektronische Communicatie.

Ten tweede stelt het Comité vast dat het begrip **“geautomatiseerde stroom van gegevens en metagegevens”** onvoldoende duidelijk maakt

Le Comité rappelle que, selon l'exposé des motifs de la loi du 30 mars 2017¹¹, *« le SGRS peut déjà intercepter des communications se déroulant exclusivement à l'étranger. »*¹²

5. Le Comité constate que le Projet introduit la notion de **« transmission automatique de flux de données et de métadonnées »**. Celle-ci est définie à l'article 1, 10° comme *« l'envoi automatisé de flux de données et de métadonnées qui ne nécessite aucune intervention humaine »*. Le Comité juge cette définition insuffisante.

Tout d'abord, cette description ne précise nulle part la notion de **« métadonnées »**. Le Comité se demande s'il s'agit ici de la même notion que celle visée à l'article 2, 93°, de la Loi sur les Communications Électroniques, où la notion de **« métadonnées de communications électroniques »** est définie comme suit : *« les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication »*. Toutefois, ni dans le préambule du Projet ni dans le rapport au Roi qui l'accompagne, un lien n'est établi entre le Projet et la Loi sur les Communications Électroniques.

Deuxièmement, le Comité constate que la notion de **« flux automatisé de données et de métadonnées »** ne précise pas suffisamment

⁵ Wet van 30 maart 2017 tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en van artikel 259bis van het Strafwetboek (BS 28 april 2017).

⁶ Parl. St. Kamer 2015-2016, nr. 54-2043/001, 82.

¹¹ Loi du 30 mars 2017 modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259bis du Code pénal (M.B. 28 avril 2017).

¹² Doc. parl. Chambre 2015-2016, n° 54-2043/001, 82.

dat ook verwezen wordt naar de **inhoud van communicatie**.

6. Artikel 9, §4 verplicht het diensthoofd van de ADIV om het Comité in kennis te stellen van het **samenwerkingsakkoord** tussen de ADIV en de betrokken dienstenverstreker/netwerkoperator, of van vervangende ministerieel besluit. Het Comité is van oordeel dat een termijn moet worden toegevoegd waarbinnen aan deze kennisgeving moet worden voldaan.

7. Artikel 11, §2 verplicht de betrokken dienstenverstreker of netwerkoperator om een **lijst** bij te houden *“van het personeel dat op de hoogte is van het bestaan van de samenwerking tussen de ADIV en de verstreker van een elektronische communicatiedienst of de netwerkoperator”*. Het Comité is van oordeel dat niet enkel het personeel *sensu stricto* op deze lijst dient opgenomen te worden, maar alle personen van de betrokken onderneming die van het bestaan van het samenwerkingsakkoord op de hoogte zijn. Dus ook leidinggevendenden zoals de CEO, bestuursleden, e.d.m.

8. Artikel 15, §3 geeft de ADIV zes maanden om een stroom van (meta)gegevens te **evalueren op hun relevantie**. Het Comité heeft geen bezwaar mocht de voorgestelde termijn éénmaal verlengbaar zijn voor 3 maanden – indachtig afdoende argumentatie en kennisgeving hiervan aan Comité I – wanneer de analyse van de geïntercepteerde gegevens, de vertaling of andere verwerkingen ervan problematisch verlopen. Indien gewenst, dient deze mogelijkheid tot verlenging in het Ontwerp opgenomen te worden.

9. Artikel 15, §3 stelt verder – in zijn tweede en vierde lid – dat “[w]anneer de gegevens en metagegevens” (tweede lid) *“niet relevant worden geacht”* / (vierde lid) *“relevant worden geacht”* *“door het diensthoofd of, in voorkomend geval, namens hem, door de directeur operaties of de daartoe aangeduide agenten”*. Het Comité is van oordeel dat, in het licht van het recentelijk goedgekeurde KB van 30 juni 2025 tot bepaling van de algemene structuur van het Ministerie van Landsverdediging en van de bevoegdheden

qu'elle fait également référence au **contenu des communications**.

6. L'article 9, § 4 oblige le Chef du SGRS à informer le Comité de l'accord de coopération conclu entre le SGRS et le fournisseur de services/opérateur du réseau concerné, ou de tout arrêté ministériel subsidiaire. Le Comité estime qu'il convient d'ajouter un délai dans lequel cette notification doit être effectuée.

7. L'article 11, § 2 oblige le fournisseur de services ou l'opérateur du réseau concerné à tenir une **liste** *« du personnel ayant connaissance de l'existence de la coopération entre le SGRS et le fournisseur d'un service de communication électronique ou l'opérateur du réseau »*. Le Comité estime que cette liste ne doit pas seulement comprendre le personnel *sensu stricto*, mais toutes les personnes de l'entreprise concernée qui ont connaissance de l'existence de l'accord de coopération. Cela inclut donc également les dirigeants tels que le CEO, les membres du conseil d'administration, etc.

8. L'article 15, § 3 accorde au SGRS six mois pour **déterminer la pertinence** d'un flux de (méta)données. Le Comité n'a aucune objection à ce que le délai proposé puisse être prolongé une fois de trois mois – moyennant une argumentation suffisante et une notification au Comité R – lorsque l'analyse des données interceptées, leur traduction ou tout autre traitement pose problème. Si souhaité, cette possibilité de prolongation doit être incluse dans le Projet.

9. L'article 15, § 3 stipule en outre, dans ses alinéas 2 et 4, que *« [l]orsque les données et métadonnées (alinéa 2) ne sont pas considérées comme pertinentes / (alinéa 4) sont considérées comme pertinentes »* *« par le dirigeant du service ou, selon le cas, en son nom, par le directeur des opérations ou les agents désignés à cet effet »*. Le Comité estime que, compte tenu de l'Arrêté royal approuvé récemment, le 30 juin 2025, définissant la structure générale du ministère de la Défense et les compétences de certaines autorités, il existe

van bepaalde autoriteiten, onduidelijkheid bestaat rond het begrip “directeur operaties”. Artikel 42 van dit KB introduceert namelijk de militaire eenheid Cyber Command binnen de ADIV, geleid door een Cyber Commander. Binnen Cyber Command bestaat er een directeur Cyber Operations. Binnen de ADIV bestaat dan weer (o.a.) een directeur Inlichtingen die verantwoordelijk is voor de inlichtingencyclus, waaronder het verzamelen en analyseren van inlichtingen. Laatstgenoemde activiteit omvat ook het nagaan van de relevantie van de ingewonnen informatie.

Naast onduidelijkheid rond de notie “directeur operaties” bestaat er ook onduidelijkheid van de (eventuele) rol van de Cyber Commander in de gehele regeling voorzien in het Ontwerp.

10. Het Ontwerp stelt dat een vernietiging van gegevens plaatsvindt door “**automatische verwijdering door overschrijving**”. Door niet enkel het betrokken bestand te verwijderen, maar door de vrijgekomen ruimte op te vullen met nieuwe data wordt inderdaad geopteerd voor een veilig wissen van gegevens. Het Comité vraagt om betrokken proces duidelijker te definiëren in het in het Staatsblad te publiceren verslag aan de Koning.

11. De burger heeft recht op een controle op de activiteiten van de inlichtingendiensten. Opdat een dergelijke controle *doeltreffend* zou kunnen zijn, moeten een aantal randvoorwaarden vervuld worden. Zo is het Comité van oordeel dat elk systeem of apparatuur dat door een inlichtingendienst gebruikt wordt voor de geautomatiseerde verwerking van (persoons)gegevens technisch moet voldoen aan de vereiste van uitlegbaarheid (in het IT-jargon beter gekend als het **principe van explainability**); en dat deze technische mogelijkheid juridisch moet worden vastgesteld. Voor wat betreft de ter advies voorgelegde regeling is het Comité van oordeel dat deze verplichting expliciet in het Ontwerp moet worden opgenomen gezien zeker de informatiegaring door middel van een geautomatiseerde stroom van (meta)gegevens de noodzaak doet opleven dat

une certaine confusion autour de la notion de « **directeur des opérations** ».

L'article 42 de cet Arrêté royal introduit en effet l'unité militaire Cyber Command au sein du SGRS, dirigée par un Cyber Commander. Au sein du Cyber Command, il y a un directeur Cyber Operations. Au sein du SGRS, il existe également (entre autres) un directeur Renseignement, qui est responsable du cycle du renseignement, y compris la collecte et l'analyse des renseignements. Cette dernière activité comprend également la vérification de la pertinence des informations recueillies.

Outre le flou qui entoure la notion de « directeur des opérations », il existe également une incertitude quant au rôle (éventuel) du Cyber Commander dans l'ensemble du dispositif prévu dans le Projet.

10. Le Projet prévoit que la destruction des données s'effectue par « **suppression automatique par réécriture** ». En ne se contentant pas de supprimer le fichier concerné, mais en remplissant l'espace libéré avec de nouvelles données, on opte en effet pour un effacement sécurisé des données. Le Comité demande que ce processus soit défini plus clairement dans le rapport au Roi qui sera publié au Moniteur belge.

11. Le citoyen a le droit de contrôler les activités des services de renseignement. Pour que ce contrôle soit *efficace*, certaines conditions préalables doivent être remplies. Ainsi, le Comité considère que tout système ou équipement utilisé par un service de renseignement pour le traitement automatisé de données (à caractère personnel) doit satisfaire techniquement à l'exigence d'explicabilité (mieux connue dans le jargon informatique sous le nom de **principe d'explainability**) et que cette possibilité technique doit être juridiquement établie.

En ce qui concerne la réglementation soumise pour avis, le Comité estime que cette obligation doit être explicitement incluse dans le Projet, étant donné que la collecte d'informations au moyen d'un flux automatisé de (méta)données rend nécessaire de pouvoir expliquer, tant a priori qu'a posteriori, comment le système est parvenu à un résultat bien déterminé. Par ailleurs, la

zowel a priori als a posteriori uitlegbaar is hoe het systeem tot een welbepaald resultaat is gekomen. Overigens is de uitlegbaarheid niet enkel belangrijk voor de externe controle op de werking en de resultaten van het systeem. Minstens even belangrijk is dat de agenten van de ADIV om operationele redenen en omwille van interne controle dit kunnen nagaan.

12. Artikel 18, §1 (Nederlandstalige versie) stelt: *“Jaarlijks wordt de samenwerking die voortvloeit uit de uitvoering van dit koninklijk besluit herzien tussen enerzijds de ADIV en de verstrekker van een elektronische communicatiedienst (...)”*. De Franstalige versie stelt: *“Une réévaluation de la coopération découlant de l’exécution du présent arrêté royal est réalisée annuellement entre d’une part, le SGRS et le fournisseur d’un service de communications électroniques ou l’opérateur du réseau (...)”*. Het is het Comité onduidelijk of het begrip “réévaluation” – zoals in het Ontwerp – vertaald moet worden als “herzien” of eerder als “geëvalueerd”. Beide begrippen dekken niet eenzelfde lading.

In dezelfde lijn wordt in art. 19 het begrip “mécanisme de réévaluation” vertaald als “herzieningsmechanisme”.

13. Artikel 19 belast het Comité met een **controleopdracht** op de samenwerking tussen de ADIV en de betrokken netwerkoperator of dienstenverstrekker. Deze bijzondere controle is driedelig. Vooreerst wordt het Comité belast met een adviesverplichting binnen de totstandkoming van een bepaald samenwerkingsakkoord. Het Comité krijgt van de auteur van het Ontwerp een termijn van 2 weken om dit advies uit te brengen. Ten tweede wordt het Comité belast met het verrichten van een controle op de uitvoering van dit samenwerkingsakkoord. Tot slot moet het Comité periodieke controles verrichten op de uitvoering door middel van het in artikel 18 bedoelde herzieningsmechanisme.

Wat betreft de controle *a priori* is het Comité van oordeel dat twee weken, indachtig de hoge mate van techniciteit van de samenwerking tussen de ADIV en de betrokken netwerkoperator of

traçabilité n'est pas seulement importante pour le contrôle externe du fonctionnement et des résultats du système. Il est au moins aussi important que les agents du SGRS puissent vérifier ces éléments pour des raisons opérationnelles et à des fins de contrôle interne.

12. Artikel 18, § 1^{er} (version néerlandaise) stipule que : *« Jaarlijks wordt de samenwerking die voortvloeit uit de uitvoering van dit koninklijk besluit herzien tussen enerzijds de ADIV en de verstrekker van een elektronische communicatiedienst (...) »*. La version française stipule que : *« Une réévaluation de la coopération découlant de l’exécution du présent arrêté royal est réalisée annuellement entre d’une part, le SGRS et le fournisseur d’un service de communications électroniques ou l’opérateur du réseau (...) »*. Le Comité ne sait pas si le terme « réévaluation » – tel qu’il apparaît dans le Projet – doit être traduit par « herzien » ou plutôt par « geëvalueerd ». Ces deux termes n'ont pas la même signification.

Dans le même ordre d'idées, à l'article 19, la notion de « mécanisme de réévaluation » est traduit par « herzieningsmechanisme ».

13. L'article 19 confère au Comité une **mission de contrôle** de la coopération entre le SGRS et l'opérateur du réseau ou le fournisseur de services concerné. Ce contrôle particulier comporte trois volets. Tout d'abord, le Comité est chargé d'émettre un avis dans le cadre de la conclusion d'un accord de coopération donné. Le Comité dispose d'un délai de deux semaines accordé par l'auteur du Projet pour rendre cet avis. Deuxièmement, le Comité est chargé de contrôler la mise en œuvre du présent accord de coopération. Enfin, le Comité doit effectuer des contrôles périodiques de la mise en œuvre au moyen du mécanisme de révision visé à l'article 18.

En ce qui concerne le contrôle *a priori*, le Comité estime que deux semaines ne suffisent pas pour rendre un avis fondé, compte tenu du caractère hautement technique de la coopération entre le

dienstenverstreker, niet realistische is om een gedegen advies uit te brengen. Voorts wenst het Comité dat er een verplichte door de ADIV uitgevoerde mondelinge toelichting aan het Comité in het Ontwerp wordt ingeschreven.

Wat betreft de voorziene periodieke controle is het voor het Comité onduidelijk welk soort controle door de auteur wordt verwacht. Het dispositief is hieromtrent weinig duidelijk, en het verslag aan de Koning licht ter zake niet verder toe.

Tot slot dient opgemerkt te worden dat het instellen van een bijzondere controleopdracht in hoofde van het Comité een bijkomend beslag zal leggen op de capaciteit van het Comité. Om het Comité in staat te stellen voldoende adequaat aan de verwachtingen en behoeften van de regering op vlak van controle te voldoen, dient het te beschikken over voldoende materiële, financiële en personele middelen. Het Comité verzoekt om hiermee rekening te houden bij het goedkeuren van het ontwerp van koninklijk besluit.

14. In het verslag aan de Koning wordt dieper ingegaan op de beperkingen en waarborgen van de onderschepte stromen van gegevens en metagegevens. Als beperkingen en waarborgen worden vermeld:

- “- de lijst van intercepties bedoeld in artikel 44/3 van de organieke wet;*
- de vooraf door de ADIV ingestelde filters om aan de voormelde lijst te voldoen;*
- de invoering van veiligheidsmaatregelen voor de overdracht, verwerking, bewaring en vernietiging van de stromen van gegevens en metagegevens;*
- de invoering van een specifieke controleprocedure door het Comité I.”.*

Het Comité adviseert om volgend streepje toe te voegen:

“de wettelijke vereisten inzake gegevensverwerking vastgelegd in de wet van 30 november 1998 en, voor wat betreft de verwerking van persoonsgegevens, in de Gegevensbeschermingswet van 30 juli 2018”.

SGRS et l'opérateur du réseau ou le fournisseur de services concerné. Le Comité souhaite en outre que le Projet prévoie une obligation pour le SGRS de lui fournir des explications orales.

En ce qui concerne le contrôle périodique prévu, le Comité ne comprend pas bien quel type de contrôle est attendu par l'auteur. Le dispositif n'est pas très clair à ce sujet et le rapport au Roi ne fournit pas d'explications supplémentaires à ce sujet.

Enfin, il convient de noter que la mise en place d'une mission de contrôle particulière au sein du Comité sollicitera davantage les capacités de celui-ci. Afin de permettre au Comité de répondre de manière adéquate aux attentes et aux besoins du gouvernement en matière de contrôle, il doit disposer de ressources matérielles, financières et humaines suffisantes. Le Comité demande que cet aspect soit pris en considération lors de l'approbation du projet d'arrêté royal.

14. Le rapport au Roi examine plus en détail les restrictions et les garanties relatives aux flux de données et de métadonnées interceptés. Les restrictions et garanties mentionnées sont les suivantes :

- « - la liste d'interception visées à l'article 44/3 de la loi organique ;*
- les filtres mis en place en amont par le SGRS pour respecter la liste précitée ;*
- la mise en place de mesures de sécurité pour la transmission, le traitement, la conservation et la destruction des flux de données et de métadonnées ;*
- la mise en place d'une procédure de contrôle spécifique par le Comité R. ».*

Le Comité recommande d'ajouter le tiret suivant :
« les exigences légales en matière de traitement des données prévues par la loi du 30 novembre 1998 et, en ce qui concerne le traitement des données à caractère personnel, par la loi du 30 juillet 2018 relative à la protection des données ».

Legistieke en taalkundige opmerkingen

15. Het begrip “verwerking” wordt in art. 1, 8° omschreven als “de verwerking zoals bepaald in artikel 26, 2° van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens”. Art. 26, 2° maakt onderdeel uit van titel 2 van de wet van 30 juli 2018 die de voorschriften bevat inzake de verwerking van persoonsgegevens door de bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten. Art. 72, §1 van de wet van 30 juli 2018 stelt dat bepaalde definities uit art. 26 van toepassing zijn op de ondertitel 1 van titel 3 van de wet van 30 juli 2018 (m.n. art. 72 tot 104) die de voorschriften bevat inzake de verwerking van persoonsgegevens door de inlichtingendiensten. Omwille van de duidelijkheid dient in art. 1, 8° Ontwerp, naast de verwijzing naar art. 26, 2°, ook verwezen te worden naar art. 72, §1 van de wet van 30 juli 2018.

16. Op twee plaatsen in het Ontwerp wordt gebruik gemaakt van een verkeerde benaming van de betrokken wet van 11 december 1998. Sinds de wet van 2 juni 2024 (BS 8 juli 2024) is de correcte benaming, de “wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst” (in: de aanhef (1x) en art. 1, 2°).

17. In de Nederlandstalige versie van artikel 11, §1 moeten de woorden “de operator van een netwerk” vervangen worden door “de netwerkoperator” (Cf. de definities vastgelegd in artikel 1 Ontwerp).

18. Artikel 12, §1 stelt: “De informatie en documenten die in het kader van deze samenwerking tussen de ADIV en de verstrekker van een elektronische communicatiedienst of de netwerkoperator worden uitgewisseld, worden van nature als gevoelig beschouwd.”. Het Comité is van oordeel dat de woorden “van nature” moeten worden geschrapt. Betrokken woorden hebben geen onmiddellijk meerwaarde. Het Comité volgt het Ontwerp in de zin dat dergelijke

Remarques légistiques et linguistiques

15. La notion de « traitement » est définie à l'article 1^{er}, 8° comme « le traitement tel que défini à l'article 26, 2° de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ». L'article 26, 2°, fait partie du titre 2 de la loi du 30 juillet 2018 qui contient les dispositions relatives au traitement des données à caractère personnel par les autorités compétentes en vue de la prévention, de l'enquête, de la détection et de la poursuite des infractions pénales. L'article 72, § 1^{er}, de la loi du 30 juillet 2018 stipule que certaines définitions de l'article 26 s'appliquent au sous-titre 1^{er} du titre 3 de la loi du 30 juillet 2018 (c'est-à-dire les articles 72 à 104) qui contient les dispositions relatives au traitement des données à caractère personnel par les services de renseignement. Dans un souci de clarté, l'article 1^{er}, 8° du Projet doit, outre la référence à l'article 26, 2°, également faire référence à l'article 72, § 1^{er} de la loi du 30 juillet 2018.

16. À deux endroits dans le Projet, une dénomination erronée de la loi concernée du 11 décembre 1998 est utilisée. Depuis la loi du 2 juin 2024 (M.B. 8 juillet 2024), la dénomination correcte est « loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé » (dans : le préambule (1x) et l'art. 1^{er}, 2°).

17. Dans la version néerlandaise de l'article 11, § 1^{er}, les mots « de operator van een netwerk » doivent être remplacés par « de netwerkoperator » (Cf. les définitions figurant à l'article 1^{er} du Projet).

18. L'article 12, § 1^{er} stipule que : « Les informations et documents échangés dans le cadre de cette coopération entre le SGRS et le fournisseur d'un service de communications électroniques ou l'opérateur du réseau sont considérés par nature comme sensibles ». À l'estime du Comité, les mots « par nature » doivent être supprimés. Ces mots n'apportent aucune valeur ajoutée immédiate. Le Comité suit le Projet en ce sens que ces données doivent être considérées comme sensibles.

gegevens als gevoelig moeten worden beschouwd.

19. In de Nederlandstalige versie van artikel 19, 2° moet het streepje in “de ADIV-intercepties” weggelaten worden om de zin te doen kloppen.

19. Dans la version néerlandaise de l'article 19, 2°, le tiret dans « de ADIV-intercepties » doit être supprimé pour que la phrase soit correcte.

Brussel, 11 september 2025

Bruxelles, le 11 septembre 2025

VOOR HET VAST COMITÉ I

POUR LE COMITÉ PERMANENT R

Vanessa SAMAIN

Voorzitster

Présidente

Frédéric Givron

Griffier

Greffier