Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 118/2025 van 12 november 2025

Betreft: advies met betrekking tot een ontwerp van koninklijk besluit houdende de regels voor de vernietiging van onwettig verkregen gegevens als bedoeld in artikel 44/4 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en houdende de regels voor samenwerking als bedoeld in artikel 44/5 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (CO-A-2025-104).

Trefwoorden: interceptie van elektronische communicatie; medewerking van operatoren en verstrekkers van elektronische-communicatiediensten; versleuteling; netwerken; nationale veiligheid; inlichtingen- en veiligheidsdiensten.

Vertaling

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, met name de artikelen 23 en 26 (hierna "WOG");

Gelet op Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (hierna "AVG");

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna "WVG");

Gelet op de adviesaanvraag van mevrouw Vanessa Matz, minister van Modernisering van de Overheid, belast met Overheidsbedrijven, Ambtenarenzaken, het Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid, ontvangen op 24 juli 2025;

Gelet op het verzoek om aanvullende informatie, gericht aan de aanvrager op 2 september 2025;

Gelet op de antwoorden van de aanvrager van 15 september 2025;

Gelet op het verzoek om aanvullende informatie, gericht aan de aanvrager op 15 september 2025;

Gelet op de antwoorden van de aanvrager van 17 september 2025;

Gelet op het verzoek van de heer Bart Preneel (hierna "de door de Autoriteit aangewezen deskundige") om als deskundige op te treden op 25 september 2025, overeenkomstig artikel 18/1 van de WOG en de artikelen 3 en 4 van het Reglement van interne orde van de Gegevensbeschermingsautoriteit;

Gelet op het verzoek om aanvullende informatie, gericht aan de aanvrager op 5 oktober 2025;

Gelet op de antwoorden van de aanvrager van 9 oktober 2025;

Gelet op de mededeling door de door de Autoriteit aangewezen deskundige van zijn verslag op 3 november 2025;

Brengt de Autorisatie- en Adviesdienst van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit") op 12 november 2025 het volgende advies uit:

I. VOORWERP EN CONTEXT VAN DE ADVIESAANVRAAG

1. De aanvrager heeft bij de Autoriteit een adviesaanvraag ingediend met betrekking tot een ontwerp van koninklijk besluit *houdende de regels voor de vernietiging van onwettig verkregen gegevens als bedoeld in artikel 44/4 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en houdende de regels voor samenwerking als bedoeld in artikel 44/5 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten* (hierna "**het ontwerp**").

2. Artikel 44/5 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (hierna "**de I&V-wet**") betreft **de medewerking van netwerkoperatoren of de verstrekkers van elektronische-communicatiediensten** in het kader van de interceptie van in het buitenland uitgezonden of ontvangen communicatie, zoals bedoeld in artikel 44 van de I&V-wet. Volgens deze laatste bepaling kan de Algemene Dienst Inlichting en Veiligheid (hierna "**de ADIV**"): "*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°*" (vetgedrukt door de Autoriteit). Deze onderscheppingen worden **voornamelijk uitgevoerd op basis van een jaarlijkse lijst van organisaties of instellingen**.

3. Artikel 44/ 5, eerste lid, van de I&V-wet bepaalt: "***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.*" (vetgedrukt door de Autoriteit) Het ontwerp voert het laatste lid van dit artikel uit, waarin staat dat de Koning, op voorstel van de minister van Defensie en de minister bevoegd voor elektronische communicatie, de nadere regels bepaalt voor de medewerking van de betrokken operator of verstrekker.

4. Samengevat voorziet het ontwerp, om de onderschepping van de gewenste elektronische communicatie (metagegevens en inhoud) te organiseren, in **een selectie gevolgd door een dubbele filtering van de gegevensstromen van elektronische communicatie**[1]. Eerst wordt een **selectie** van gegevensstromen gemaakt via apparatuur die op de netwerkinfrastructuur van de betrokken operator of verstrekker is geplaatst, en vervolgens worden deze stromen gedupliceerd naar apparatuur van de ADIV die "bij" deze operator of verstrekker is geïnstalleerd. Een **eerste filtering** van deze communicatiestromen wordt uitgevoerd via deze apparatuur. Een **tweede**, nauwkeurigere **filtering** van de doorgegeven gegevens vindt dan plaats in de installaties van de ADIV zelf.

5. De bovengenoemde bepalingen zijn in de I&V-wet opgenomen door de wet van 30 maart 2017 *tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst en van artikel 259bis van het Strafwetboek* (hierna "**wet van 2017**")[2]

6. De toenmalige ontwerpbepalingen van de wet van 2017 waren het voorwerp van advies nr. 20/2016 van de Commissie voor de bescherming van de persoonlijke levenssfeer van 18 mei 2016 *over een voorontwerp van wet tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst* (CO-A-2016-016) (hierna "**het advies van de CBPL van 2016**"),

---

[1] Zie de punten 55 en 61.

[2] In de memorie van toelichting bij deze wet wordt met betrekking tot het onderscheppen van elektronische communicatie met name vermeld:

"*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 taping"*

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 taping 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 afluisterplan, 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.", Parl. St., Kamer van volksvertegenwoordigers, nr. 54-2043/001, p. 89.

een advies van het Vast Comité I *over het wetsontwerp tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (I&V-wet) (2017)*[3] (hierna "**het advies van het Comité I van 2017**") en advies nr. 59.509/4 van de Raad van State van 27 juni 2016 *over een voorontwerp van wet tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst* (hierna "**het advies van de Raad van State van 2016**"). Toen het onderhavige advies werd opgesteld, bracht het Comité I **advies nr. 002/CPR/2025 van 11 september 2025** over het ontwerp uit (hierna "**het advies van het Comité I**")[4].

7. Het is duidelijke dat de Autoriteit bevoegd is voor de verwerking van gegevens die onder de verantwoordelijkheid vallen van de operatoren van telecommunicatienetwerken en de verstrekkers van elektronische-communicatiediensten, ongeacht of deze rechtstreeks verband houden met de verwerking van persoonsgegevens door de ADIV, dat wil zeggen vallend onder titel 3 van de WVG[5].

II. ONDERZOEK VAN HET ONTWERP

Dit advies is als volgt opgebouwd:

---

[3] Dit advies is beschikbaar via de link https://www.comiteri.be/index.php/nl/publicaties/adviezen, laatstelijk geraadpleegd op 29/08/2025. Voor het opstellen van haar advies had de CBPL inzage gekregen in het advies van het Comité I, dat niet openbaar was (« *Beperkte verspreiding (K.B. 24 maart 2000)* »).

[4] Dit advies is beschikbaar via de link https://www.comiteri.be/index.php/nl/publicaties/adviezen, laatstelijk geraadpleegd op 20/10/2025. De aanvrager heeft aangegeven dat het advies van de Raad van State aan het einde van het proces zal worden gevraagd, zodra het ontwerp is geconsolideerd op basis van de adviezen van de Autoriteit en het Comité I en het advies dat in het kader van de openbare raadpleging is ontvangen.

[5] Zie bijvoorbeeld advies nr. 184/2021 van 4 oktober 2021 *met betrekking tot een voorontwerp van wet tot wijziging van de wet van 10 juli 2006 betreffende de analyse van de dreiging (CO-A-2021-174)*, over instellingen die geen inlichtingen- en veiligheidsdiensten zijn, en advies nr. 34/2024 van 15 april 2024 *betreffende een wetsvoorstel tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en de wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten (CO-A-2024-139).* Wat betreft de verschillende normatieve kaders op het gebied van gegevensbescherming, zie Gegevensbeschermingsautoriteit, Autorisatie- en Adviesdienst, beschikbaar via de link https://www.gegevensbeschermingsautoriteit.be/publications/brochure-publieke-sector-en-wettelijke-bepalingen.pdf, laatstelijk geraadpleegd op 01/09/2025., pp. 9-11.

Zie **punt 41**.

II.1 Het advies van de CBPL van 2016

8. **In 2016 had de Commissie voor de bescherming van de persoonlijke levenssfeer**, de voorloper van de Autoriteit, **in haar advies (punten 25 tot en met 37) kritiek geuit op het voorontwerp van wet dat aanleiding gaf tot de wet van 2017**, met betrekking tot de interceptie van in het buitenland uitgezonden of ontvangen elektronische communicatie, en de medewerking van de betrokken dienstverstrekkers op dit gebied.

9. Bij wijze van inleiding vermeldt de Autoriteit hieronder de meest relevante overwegingen ter zake:

> "*B.5 Uitbreiding van de voorrechten van de ADIV in het buitenland*
>
> *B.5.1 Nieuwe ad hoc methoden*
> *(artikelen 79 en 80 van het voorontwerp tot wijziging van de artikelen 44bis en ter van de WIV)*
>
> *25 In de marge van de specifieke en uitzonderlijke inlichtingenmethoden is de ADIV onder meer bevoegd voor een ad hoc methode die toelaat om in het buitenland uitgezonden communicaties te onderscheppen, en dit onder bepaalde voorwaarden en mits een ad hoc controle (artikelen 259 bis §5 van het Strafwetboek en 44 bis en ter van de WIV). De onderscheppingen gebeuren volgens een jaarlijks afluisterplan dat een lijst behelst van de organisaties en instellingen die het onderwerp zullen zijn van intercepties en dat is goedgekeurd door de minister van Defensie en overgezonden aan het Comité I.*
>
> *26* […]
>
> *27. Hij wenst **deze grotere flexibiliteit in te voeren** voor deze twee methoden van informatievergaring **omdat** de ADIV niet in staat is om de vastgestelde procedure voor het gebruik van specifieke en uitzonderlijke methoden te volgen om verschillende redenen: in het buitenland, tijdsverschil, hoogdringendheid, geen enkel beveiligd communicatiemiddel, onmogelijkheid om zich te richten op een specifieke persoon of gebeurtenis, ...*

28. De aanvrager voorziet evenwel om de ad hoc controle te versterken, met name door een meer ontwikkelde motivering van de jaarlijkse lijst en door de maandelijkse overzending aan het Comité I van een gemotiveerde lijst met landen of organisaties en instellingen die het voorwerp zijn geweest van een afluistering, intrusie of beeldopnames. Zo zou het Comité I op regelmatige wijze op de hoogte worden gehouden van de uitgevoerde afluisteringen, intrusies en beeldopnames.

29 De Commissie herinnert eraan dat de intrusie in een informaticasysteem en de opname van beelden in principe onderworpen zijn aan de administratieve controle van de BIM-commissie en de rechterlijke controle door het Comité I. Het voorontwerp zal deze methoden aan deze controles onttrekken om ze te onderwerpen aan een ***minder uitgebreide ad hoc controle****.*

30. Zij merkt eveneens op dat deze maatregelen niet gericht zijn of althans waarvan het niet de bedoeling is deze te cibleren op geïdentificeerde personen maar op organisaties en groeperingen. Het moge evenwel duidelijk zijn dat de drie bedoelde inlichtingenmethoden onvermijdelijk persoonsgegevens zullen capteren.

31. Bijgevolg formuleert zij ***voorbehoud bij de geplande uitbreiding van een ad hoc procedure die van nature beperkt zou moeten blijven****.*

B.5.2 Uitbreiding van de mogelijkheid tot interceptie van communicatie tot de communicaties ontvangen in het buitenland
(artikel 76 van het voorontwerp tot (her)invoering van artikel 44 van de WIV)

32. In het raam van de hiervoor vermelde methode voor onderschepping door de ADIV van elke vorm van in het buitenland uitgezonden communicatie, beoogt het voorontwerp de ***uitbreiding van deze methode tot de in het buitenland ontvangen communicaties****.*

33. Volgens de memorie van toelichting vindt deze aanpassing plaats als gevolg van de technologische evoluties die onder meer gebaseerd zijn op het IP protocol. Het basiscriterium dat traditioneel gevormd werd door de oorsprong van de communicatie, is dus niet langer bruikbaar.

34. De Commissie neemt akte van deze toelichting maar stelt vast dat de prerogatieven, en bijgevolg ***de intrusiemogelijkheden in het privéleven van de betrokkenen, die aan***

de ADIV worden verleend hiermee sterk worden uitgebreid, vermits ook communicatie die uitsluitend in het buitenland plaatsvindt zal kunnen onderschept worden*.*

B.5.3 Invoering van een medewerking van de netwerkoperatoren in het buitenland (artikel 81 van het voorontwerp tot invoering van een nieuw artikel 44/5 van de WIV)

35. Hoewel de medewerking van de netwerkoperatoren voorzien is voor de toepassing van de specifieke en uitzonderlijke methoden, is dit niet het geval voor de uitzonderlijke methode van interceptie van in het buitenland ontvangen (of uitgezonden) communicaties. ***De inlassing van dit nieuwe artikel 44/5 heeft tot doel te voorzien in deze verplichte medewerking*** *van de netwerkoperatoren en verstrekkers van telecommunicatiediensten die (eveneens) elektronische-communicatiediensten aanbieden op het Belgisch grondgebied.*

36. ***Het is de bedoeling van de aanvrager om de ADIV toe te laten over te gaan tot wat men "cable tapping" noemt*** *en dus alle communicaties te onderscheppen die via de kabels verloopt.*

37. De Commissie staat ***afkerig tegen een dergelijke werkwijze die de ADIV zou toelaten een gegevensstroom te onderscheppen die buitensporig is in het licht van het beoogde doeleinde en over te gaan tot datamining, wat begint te lijken op massabewaking. Het heeft in dit verband weinig belang of die gegevensstromen door de ADIV zouden gefilterd worden op basis van een afluisterplan teneinde daaruit enkel de in het buitenland uitgezonden communicaties en gegevens te halen, die door dit plan en in verband met de opdrachten van de ADIV, zijn toegestaan. In tegenstelling tot wat in de toelichting vermeld staat laat de wettekst op zich wel degelijk toe dat aan massacaptatie wordt gedaan.***" (vetgedrukt door de Autoriteit)

II.2 Het betreffende geval

II.2.1 De betrokken opdrachten van de ADIV

10. Zoals de Raad van State tweemaal heeft benadrukt, worden de **inlichtingenopdrachten zeer ruim gedefinieerd in de artikelen 7, 8 en 11 van de I&V-wet, zodat zij bedachtzaam** en met strikte inachtneming van de beginselen van subsidiariteit en evenredigheid **moeten worden geïnterpre-**

teerd wanneer het gaat om het gebruik van specifieke en uitzonderlijke methoden voor het verzamelen van gegevens[6]. In het onderhavige geval kan de interceptie[7] van elektronische communicatie in het buitenland door de ADIV plaatsvinden in het kader van de **opdrachten bedoeld in artikel 11, § 1, 1° tot 3° en 5° van de I&V-wet**. Opgemerkt moet worden dat de wet van 2017 niet alleen specifieke bepalingen bevat met betrekking tot de uitvoering van de taken van de ADIV, maar ook de bevoegdheden van deze dienst heeft uitgebreid.

11. De onder het positief recht vallende opdrachten met betrekking tot de interceptie van elektronische communicatie zijn de volgende:

> "1° *het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de factoren die de nationale en internationale veiligheid beïnvloeden of kunnen beïnvloeden in die mate dat de Krijgsmacht betrokken is of zou kunnen worden om inlichtingensteun te bieden aan hun lopende of eventuele komende operaties, alsook de inlichtingen die betrekking hebben op elke activiteit die:*
> *a) de onschendbaarheid van het nationaal grondgebied of de bevolking,*
> *b) de militaire defensieplannen,*
> *c) het wetenschappelijk en economisch potentieel met betrekking tot de actoren, zowel de natuurlijke als de rechtspersonen, die actief zijn in de economische en industriële sectoren die verbonden zijn met defensie en die opgenomen zijn in een op voorstel van de minister van Justitie en de minister van Landsverdediging door de Nationale Veiligheidsraad goedgekeurde lijst,*
> *d) de vervulling van de opdrachten van de strijdkrachten,*
> *e) de veiligheid van de Belgische onderdanen in het buitenland,*
> *f) elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van de Nationale Veiligheidsraad,*
> *bedreigt of zou kunnen bedreigen en er de bevoegde ministers onverwijld over inlichten alsook de regering, op haar verzoek, advies te verlenen bij de omschrijving van haar binnen- en buitenlands beleid inzake veiligheid en defensie;*
>
> *2° het zorgen voor het behoud van de militaire veiligheid van het personeel dat onder de Minister van Landsverdediging ressorteert, de militaire installaties, wapens en wapensystemen, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen en, in het kader van de cyberaanvallen op wapensystemen, militaire informatica- en verbindingssystemen of systemen die de Minister van*

---

[6] Zie het advies van de Raad van State nr. 42.178/2 van 19 februari 2007 *over een voorontwerp van wet 'betreffende de methodes voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten'*.

[7] De bevoegdheid van de ADIV beperkt zich niet tot interceptie, zie punt 2.

Landsverdediging beheert, de aanval neutraliseren en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het recht der gewapende conflicten;

2° /1 het neutraliseren, in het kader van een nationale cybersecurity crisis, van een cyberaanval op informatica- en verbindingssystemen niet beheerd door de minister van Landsverdediging en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het internationaal recht;

3° het beschermen van het geheim dat, krachtens de internationale verbintenissen van België of teneinde de onschendbaarheid van het nationaal grondgebied en de vervulling van de opdrachten van de strijdkrachten te verzekeren, verbonden is met de militaire installaties, wapens, munitie, uitrusting, met de plannen, geschriften, documenten of andere militaire voorwerpen, met de militaire inlichtingen en verbindingen, alsook met de militaire informatica- en verbindingssystemen of die systemen die de Minister van Landsverdediging beheert;

[…]

5° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied"[8]*.*

12. In overeenstemming met het standpunt van de Raad van State en rekening houdend met de inmenging die wordt veroorzaakt door de artikelen 44 en 44/5 van de I&V-wet (en nog meer door de voorgestelde regeling, onverminderd latere opmerkingen over de wettelijke basis en de waarborgen die deze regeling omkaderen), is de Autoriteit van mening dat **bij de uitvoering** van deze bepalingen en **de medewerking van operatoren en verstrekkers van elektronische-communicatiediensten, de opdrachten van de <u>ADIV bedachtzaam en met strikte inachtneming van de beginselen van subsidiariteit en evenredigheid moeten worden geïnterpreteerd</u>.**

<u>II.2.2 Dienstenaanbieders die onder de verplichting tot medewerking vallen</u>

13. De Autoriteit wijst er in de eerste plaats op dat, zoals in de memorie van toelichting bij de wet van 2017 wordt aangegeven, **de soorten elektronische-communicatiediensten** waarop de wet betrekking heeft, divers en talrijk zijn, zodat ook de aanbieders die mogelijk met de ADIV moeten sa-

[8] Artikel 11, § 2, van de I&V-wet definieert bepaalde begrippen die in deze bepaling worden gebruikt.

menwerken, divers en talrijk zijn. Wat de territoriale bevoegdheid betreft, zijn dienstenaanbieders bovendien aan de regeling onderworpen **zodra zij hun diensten in België aanbieden**. Meer specifiek vermeldt de bovengenoemde toelichting het volgende:

> *"In het ontwerp wordt een definitie van "verstrekker van een elektronische-communicatiedienst" ingevoerd (nieuw 11°/1) om het personele en territoriale toepassingsgebied van de medewerkingsplicht van de telecomsector af te bakenen:*
>
> - *niet alleen de klassieke verstrekkers van een elektronische-communicatiedienst, zoals bedoeld in artikel 2, 5° van de wet van 13 juni 2005 betreffende de elektronische communicatie, vallen onder de medewerkingplicht (**Proximus, Mobistar, Base, Telenet, Scarlet, VOO, Mobile Vikings, aanbieders van gratis Wifi-hotspots …**),*
> - *maar ook **alle aanbieders van alternatieve communicatiediensten zoals Yahoo, Hotmail, Gmail, Skype, Whats App, Viber, games met chatmogelijkheid…***
>
> *Als verstrekker wordt dan ook beschouwd éénieder die een dienst verschaft die erin bestaat dat hij zijn klanten een gelegenheid geeft tot elektronische uitwisseling van informatie.*
>
> *Wat het territoriale toepassingsgebied betreft, moet erop gewezen worden dat de medewerkingsplicht van toepassing is op éénieder die een communicatiedienst aanbiedt in België. Het is bijgevolg niet vereist dat de aanbieder fysiek aanwezig is op Belgisch grondgebied.*
>
> *De definitie die in de wet wordt ingevoerd is overgenomen uit het arrest van het Hof van beroep van Antwerpen van 20 november 2013 waarin werd geoordeeld dat Yahoo een verstrekker van een elektronische-communicatiedienst in de zin van artikel 46bis van het Wetboek van Strafordering is (het equivalent van het*
>
> *artikel 18/7 van de wet op de inlichtingen- en veiligheidsdiensten) en aan de Belgische wetgeving onderworpen is omdat het zijn diensten beschikbaar stelt in België. Deze uitspraak werd op 1 december 2015 bevestigd door het Hof van Cassatie."*[9]

14. Naast verstrekkers van elektronische-communicatiediensten worden ook, meer 'klassiek', **netwerkoperatoren** beoogd, namelijk entiteiten die een elektronische-communicatienetwerk aanbieden zoals gedefinieerd in artikel 2, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie[10].

---

[9] *Parl. St.*, Kamer van volksvertegenwoordigers, nr. 54-2043/001, p. 26-27.

[10] Namelijk "*de transmissiesystemen, al dan niet gebaseerd op een permanente infrastructuur of gecentraliseerde beheercapaciteit, en in voorkomend geval de schakel- of routeringsapparatuur en andere middelen, waaronder netwerkelementen die niet actief zijn, die het mogelijk maken signalen over te brengen via draad, radiogolven, optische of andere elektromagnetische middelen waaronder satellietnetwerken, vaste (circuit- en pakketgeschakelde, met inbegrip van internet) en mobiele netwerken, elektriciteitsnetten voor zover deze voor overdracht van andere signalen dan die voor audiovisuele en auditieve mediadiensten worden gebruikt*".

Om binnen het territoriale toepassingsgebied van de betrokken samenwerking te vallen, volstaat het dat deze operatoren hun diensten in België aanbieden.

15. Op vraag van de Autoriteit heeft de aanvrager **bevestigd dat alleen de interceptie van elektronische communicatie <u>via deze in België toegankelijke diensten is toegestaan</u>**, en niet via andere diensten die eventueel door de betrokken verstrekker of operator worden aangeboden. Dit **moet worden verduidelijkt in het dispositief** van het ontwerp. Met andere woorden, als een dienstverstrekker bijvoorbeeld een dienst van type A (internettoegang) in het buitenland aanbiedt, maar een andere dienst van type B (e-mail) in België, kan hij niet worden verplicht om met de ADIV samen te werken voor zijn dienst van type A. Er kan dus **<u>geen</u> medewerking worden gevraagd** van een operator of verstrekker van elektronische-communicatiediensten **voor een dienst** (elektronische communicatie of een netwerk) **die uitsluitend buiten België wordt aangeboden, <u>ondanks</u>** het feit dat de betrokken aanbieder andere diensten (elektronische communicatie of een netwerk) in België aanbiedt.

16. In de zojuist geschetste context is de **locatie van de installaties van de betrokken dienstenaanbieders** niet onbelangrijk, aangezien het ontwerp voorziet dat de **<u>ADIV zelf apparatuur "bij" deze aanbieders zal installeren</u> en hen zal bezoeken**. In dit kader lijkt de invoering van de samenwerking haalbaar wanneer de betrokken operator of verstrekker over installaties in België beschikt, maar de Autoriteit heeft de aanvrager gevraagd hoe in de praktijk zal worden gezorgd voor toegang van de ADIV tot installaties van operatoren en verstrekkers in het buitenland, en voor de installatie van apparatuur bij hen. De aanvrager antwoordde: ***"Als de operator/verstrekker geen infrastructuur (telecommunicatie of kantoren) in België heeft, zal er geen samenwerking zijn.*** *Anders zal de samenwerking plaatsvinden zoals beschreven in het ontwerp van koninklijk besluit."* (vrij vertaald, zoals alle antwoorden van de aanvrager in dit advies) (vetgedrukt door de Autoriteit) In zijn antwoorden op het derde verzoek om aanvullende informatie van de Autoriteit, verklaarde de aanvrager: *"De medewerking van verstrekkers/operatoren vereist dat de diensten op het nationale grondgebied beschikbaar zijn* ***<u>en dat er dus een infrastructuur in België aanwezig is</u> (zelfs als deze door de verstrekker of operator wordt gehuurd of gedeeld).*** *De communicatie die het voorwerp uitmaakt van de samenwerking tussen de verstrekker of operator en de ADIV zou in dat geval worden doorgestuurd naar de installaties in België."* (vetgedrukt en onderstreept door de Autoriteit)

17. De Autoriteit is dan ook van mening dat het **dispositief van het ontwerp moet worden aangepast en alleen gericht moet zijn op samenwerking met operatoren en verstrekkers van elektronische-communicatiediensten <u>die hun diensten in België aanbieden en daartoe gebruikmaken van een technische infrastructuur die relevant is voor de betrokken dienst of het</u>**

betrokken netwerk, op het Belgisch grondgebied en waarover zij voldoende controle uitoefenen, in het licht van de voorgenomen samenwerking. In zijn verslag wijst ook de door de Autoriteit aangewezen deskundige op het volgende: "*Aangezien er apparatuur van ADIV bij de operator moet geplaatst worden, is de duplicatie enkel mogelijk als de aanbieder van elektronische-communicatiediensten of de operator over een fysieke infrastructuur op het Belgisch grondgebied beschikt* ***waarover hij voldoende controle heeft***." (vetgedrukt door de Autoriteit) Voor het overige neemt de Autoriteit, wat de betrokken soorten diensten betreft, er nota van dat de beoogde samenwerking bedoeld is om **op grote schaal te worden toegepast op iedereen die een dienst verleent waarbij de klanten de mogelijkheid wordt geboden om elektronisch informatie uit te wisselen.**

II.2.3 "Ontcijfering" van communicatie – versleuteling

18. In de memorie van toelichting van de wet van 2017 staat: "*De medewerking heeft onder andere tot doel de ADIV in staat te stellen om zijn uitrustingen in de vestiging van de operator te installeren en de interceptie mogelijk te maken, onder meer via terbeschikkingstelling van bandbreedtes en routering van stromen,* ***maar heeft ook tot doel de ADIV bij te staan bij de ontcijfering van de communicaties***." [11] (vetgedrukt door de Autoriteit) **Artikel 44/5 van de I&V-wet heeft echter alleen tot doel de "*interceptie*"** van elektronische communicatie **"*mogelijk te maken*"**.

19. De Autoriteit heeft de aanvrager verzocht te bevestigen dat het ontwerp niet gericht is op de medewerking van operatoren en verstrekkers om **elektronische communicatie te ontcijferen.** Hij antwoordde het volgende op het eerste verzoek om aanvullende informatie van de Autoriteit:

> "***De samenwerking zoals beschreven in artikel 44/5*** *van de wet van 30 november 1998 heeft betrekking op de werking van het communicatienetwerk van de verstrekker/operator, waardoor de ADIV alle vormen van in het buitenland uitgezonden of ontvangen communicatie, kan* ***opsporen, onderscheppen, afluisteren, er kennis van kan nemen en kan opnemen****. Deze bepaling heeft dus betrekking op de technische handelingen die de ADIV in staat stellen om communicatie die via de netwerken van de operator of de verstrekker verloopt, te onderscheppen, af te luisteren en op te nemen, met inbegrip van de installatie van apparatuur, het ter beschikking stellen van bandbreedte of de routering van stromen. Daarentegen l****egt zij geen algemene verplichting tot bijstand bij het ontcijferen op, met name wanneer de communicatie van begin tot eind wordt versleuteld door middelen die buiten de verstrekkers om worden gebruikt. Beperkte bijstand kan echter worden***

[11] Blz. 90.

> ***overwogen wanneer de verstrekker zelf de versleuteling toepast en over de middelen beschikt om deze op te heffen, wat nog steeds past in de logica van "interceptie mogelijk maken" in technische zin.*** *Concluderend kan worden gesteld dat h****et ontwerp geen algemene verplichting voor operatoren of verstrekkers bevat om mee te werken aan het ontcijferen van elektronische communicatie, tenzij dit rechtstreeks voortvloeit uit hun eigen versleutelingsmechanismen.***" (vetgedrukt en onderstreept door de Autoriteit)

20. Deze bepaling geeft aanleiding tot de vijf volgende opmerkingen. **Ten eerste** wijst de Autoriteit erop dat de artikelen 44 en 44/5 van de I&V-wet, die bij dezelfde wet zijn ingevoegd, duidelijk verschillende begrippen betreffen. Terwijl artikel 44 de ADIV ruime bevoegdheden toekent voor het *"opsporen, onderscheppen, afluisteren, kennis namen van en opnemen*" van bepaalde communicatie, heeft artikel 44/5 van de I&V-wet alleen betrekking op de medewerking van de operator of dienstverstrekker "*indien een ingreep in een communicatienetwerk noodzakelijk is om de* ***interceptie*** *van* [deze] *communicatie mogelijk te maken*". (vetgedrukt door de Autoriteit) **Met andere woorden, de Autoriteit is van mening dat de door de aanvrager voorgestelde interpretatie vragen oproept: de medewerking van de operator is immers beperkt tot de interceptie van communicatie.** Opmerking: in de zin van de interpretatie die door de Autoriteit wordt gevolgd, maakt artikel 18/7 van de I&V-wet ook een onderscheid tussen het "*onderscheppen*" van elektronische communicatie en het "*kennisnemen*" ervan, en verwijst het in het algemeen naar de noodzaak van de medewerking van een operator of verstrekker van elektronische-communicatiediensten in deze context (zonder specifiek te verwijzen naar een van beide verwerkingshandelingen).

21. **Ten tweede** geeft de aanvrager aan dat medewerking aan het ontsleutelen "*nog steeds past i****n de logica van "interceptie mogelijk maken' in technische zin***" (vetgedrukt door de Autoriteit), **zonder echter uit te leggen waarom interceptie ontsleuteling nodig zou maken en van welke gegevens**. In dit verband zou elektronische communicatie moeten kunnen worden onderschept zonder dat de inhoud ervan wordt ontcijferd. **Het is niet vanzelfsprekend wat betreft de voorspelbaarheid van de toepasselijke norm dat de interceptie van een communicatie het ontcijferen van gegevens inhoudt, en van welke gegevens.** De ADIV is overigens vrij om, zodra een communicatie is onderschept, met behulp van de rechtmatige en technische middelen en methoden waarover hij beschikt, een manier te zoeken om deze te ontcijferen of om in de toekomst de versleuteling van de communicatie tussen de betrokken partijen te omzeilen. De volgende overwegingen kunnen worden overgenomen uit een arrest van 13 februari 2024, *Podchasov t. Russia*, zaak nr. 33696/19, van het EHRM met betrekking tot berichtendienst Telegram:

- Een uittreksel van een verslag van het Bureau van de Hoge Commissaris van de Verenigde Naties voor de Mensenrechten bepaalt met name: "*Such alternative measures include improved, better-resourced traditional policing, undercover operations, metadata analysis and strengthened international police cooperation*" (punt 28 van het arrest);

- Een gezamenlijke verklaring van Europol en ENISA luidt: « […] *The good news is that the information needs to be unencrypted at some point to be useful to the criminals. This creates opportunities for alternatives such as undercover operations, infiltration into criminal groups, and getting access to the communication devices beyond the point of encryption, for instance by means of live forensics on seized devices or by lawful interception on those devices while still used by suspects. Moreover, forensic methods that make use of physical fingerprints of devices might not help to intercept the communication content itself, but might provide other important clues for the investigator. Even so, there are cases in which there are no such alternatives and access to the concealed content can only be gained by a form of decryption*. […] *When circumvention is not possible yet access to encrypted information is imperative for security and justice, then feasible solutions to decryption without weakening the protective mechanisms must be offered, both in legislation and through continuous technical evolution. For the latter, the fostering of close cooperation with industry partners, as well as the research community with expertise in crypto-analyses for the breaking of encryption where lawfully indicated, is strongly advised. We are convinced that a solution that strikes a sensible and workable balance between individual rights and protection of EU citizen's security interests can be found. In this respect, the deployment of European R&D instruments may drive this collaboration while at the same time EU Agencies can work closely together in establishing best practices* » (punt 33 van het arrest) ;

- Het European Information Society Institute verklaart het volgende: "*EISI also submitted that less intrusive targeted alternatives to combat crime and protect national security existed, such as, among other things, using live forensics on seized devices, guessing or obtaining private keys held by parties to the communication, using vulnerabilities in the target's software or sending an implant to targeted devices. While indiscriminate backdoors might be cheaper for the State than alternative investigative measures, they were expensive for society at large on account of the security risks they produced. The fact that the alternative methods were significantly more difficult to use on a large scale on account of their labour intensiveness, cost and logistical complexity should be viewed positively as hurdles forcing the prioritisation and targeting of measures*." (punt 47 van het arrest).

22. Dit gezegd zijnde, **merkt de Autoriteit op dat de stand van de techniek op dit gebied niet is geëvolueerd en dat het in veel gevallen nog steeds niet mogelijk is om de versleuteling**

van elektronische communicatie op te heffen <u>zonder het betrouwbaarheidsniveau van de techniek te verzwakken</u> voor gebruikers die niet betrokken zijn bij de te realiseren ontsleuteling. In dit verband verklaarde de door de Autoriteit aangewezen deskundige het volgende:

> "*Het is **belangrijk om te verduidelijken in welke mate men geëncrypteerde informatie wil decrypteren**. Op onze vraag tot verduidelijking heeft de aanvrager geantwoord dat het enkel gaat om encryptie op verbindingen tussen apparaten van de aanbieder van diensten of de operator zelf; in dit geval beschikken de aanbieder dan wel de operator over de sleutels en kunnen ze deze decrypteren. Hierbij **moet er dan wel voor gezorgd worden dat dit geen verzwakking van de beveiliging inhoudt voor andere gebruikers of dat gegevens die niet het doelwit zijn ook zouden gedecrypteerd worden. Het voorstel zou dan ook expliciet moeten vermelden dat er nooit decryptie zal gevraagd worden van informatie die "end-to-end" vercijferd is of informatie die vercijferd is in de applicatielaag**.*
>
> *Hierbij is het belangrijk om op te merken dat **alle academische experten het erover eens zijn dat het er geen technische oplossingen bestaan die toegang geven tot geëncrypteerde gegevens zonder de bescherming die encryptie kan bieden ernstig te verzwakken**[12]. Het joint statement [13]van Europol en ENISA van 23 mei 2015 beweert dat het wel mogelijk is ("We are convinced that a solution that strikes a sensible and workable balance between individual rights and protection of EU citizen's security interests can be found"), maar 10 jaar later is er nog steeds geen technische oplossing gevonden die dit doel zelfs maar ten dele bereikt (er zijn wel een aantal systemen voorgesteld in de wetenschappelijke literatuur die proberen om dit te bereiken, maar geen enkel is effectief en haalbaar). Ook **zijn alle experten het erover eens dat de digitale maatschappij enkel maar effectief kan beschermd worden als we de digitale infrastructuur beschermen met sterke encryptie*** » (vetgedrukt en wijziging van de nummering van de voetnoten door de Autoriteit).

23. **Ten derde** benadrukt de Autoriteit dat een **<u>zeer breed scala aan diensten</u>** onder de medewerkingsverplichting van artikel 44/5 van de I&V-wet valt. Het gaat dus duidelijk niet alleen om internetproviders: ook aanbieders van **'*over-the-top*'-diensten**, zoals e-mail- en berichtendiensten, vallen

---

[12] « *Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield "Whit" Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter, and Daniel J. Weitzner, Keys Under Doormats. Mandating insecurity by requiring government access to all data and communications, https://cacm.acm.org/opinion/keys-under-doormats/* ».

[13] « *https://www.enisa.europa.eu/news/enisa-news/enisa-europol-issue-joint-statement* ».

hieronder[14]. Ter herinnering: de I&V-wet en het ontwerp zijn gericht op "*éénieder die een dienst verschaft die erin bestaat dat hij zijn klanten een gelegenheid geeft tot elektronische uitwisseling van informatie*." Zo is enerzijds het **onderscheid dat de aanvrager maakt** tussen de versleutelingsmaatregelen van de operator of verstrekker en andere versleutelingsmaatregelen **minder relevant** in een context waarin **het dispositief van de I&V-wet op de verschillende niveaus van diensten van toepassing is.** Anderzijds zou het dispositief van de I&V-wet dus **een grotere impact kunnen hebben op de mogelijke verzwakking van de versleuteling op het gebied van elektronische communicatie** in het algemeen.

24. **Ten vierde**, in verband met het vorige punt, kunnen **noch de normatieve bepalingen van de I&V-wet, noch de aanvullende informatie die door de aanvrager is verstrekt, worden gebruikt om te <u>bepalen welke impact</u>** de medewerking aan het ontcijferen kan hebben **op de eigenschappen van de technologie voor het versleutelen van de communicatie van de gebruikers van de betrokken diensten *in het algemeen*** (d.w.z. de impact op andere gebruikers die niet betrokken zijn bij de opdrachten van de ADIV). Met andere woorden, kan (moet) de beoogde medewerking worden beperkt tot de uitvoering van maatregelen die geen impact hebben op de betrouwbaarheid van de versleuteling die is ingesteld voor de communicatie van gebruikers wier communicatie niet wordt onderschept, of kan deze in het algemeen de gebruikte versleutelingstechnologie kwetsbaarder maken doordat deze kwetsbaarder wordt (ten opzichte van legitieme actoren)? **Dit is een fundamenteel punt waar ook op werd gewezen door de door de Autoriteit aangewezen deskundige[15]**. Met name wijst de Autoriteit op de punten 77-78 van het arrest van 13 februari 2024, Podchasov t. Rusland, zaak nr. 33696/19 waarin het EHRM als volgt oordeelde:

> « *77. As noted above (see paragraph 57 above), it appears that in order to enable decryption of communications protected by end-to-end encryption, such as communications through Telegram's "secret chats", it would be necessary **to weaken encryption for all users**. These measures allegedly cannot be limited to specific individuals and would affect everyone indiscriminately, including individuals who pose no threat to a legitimate government interest. Weakening encryption by creating backdoors would apparently make it technically possible to perform routine, general and indiscriminate surveillance of personal electronic communications. Backdoors may also be exploited by criminal networks and would seriously compromise the security of all users' electronic communications. The Court takes note of the dangers of restricting encryption described by many experts in the field (see, in particular, paragraphs 28 and 34 above).*

[14] Zie de punten 13-16.

[15] Zie punt 22.

78. The Court accepts that encryption can also be used by criminals, which may complicate criminal investigations (see Yüksel Yalçınkaya v. Türkiye [GC], no. 15669/20, § 312, 26 September 2023). However, ***it takes note in this connection of the calls for alternative "solutions to decryption without weakening the protective mechanisms, both in legislation and through continuous technical evolution****" (see, on the possibilities of alternative methods of investigation, the Joint Statement by Europol and the European Union Agency for Cybersecurity, cited in paragraph 33 above, and paragraph 24 of the Report on the right to privacy in the digital age by the Office of the United Nations High Commissioner for Human Rights, cited in paragraph 28 above; see also the explanation by third-party interveners in paragraph 47 above).*

79. The Court concludes that ***in the present case the ICO's statutory obligation to decrypt end-to-end encrypted communications risks amounting to a requirement that providers of such services weaken the encryption mechanism for all users; it is accordingly not proportionate to the legitimate aims pursued***. » (vetgedrukt door de Autoriteit)

25. **Ten vijfde** verwijst de Autoriteit in het algemeen naar haar recente **advies nr. 16/2025 van 27 maart 2025 op eigen initiatief betreffende het Verdrag van de Verenigde Naties tegen cybercriminaliteit** (CO-A-2025-019), waarin zij met name in punt 23 aanbeveelt **het Hof van Justitie te verzoeken een advies uit te brengen** over de verenigbaarheid met de Europese Verdragen van artikel 28.4 van het Verdrag van de Verenigde Naties tegen cybercriminaliteit[16], dat eveneens betrekking heeft op de problematiek in kwestie[17]. En zij benadrukt nogmaals[18] het belang van het behoud van encryptie. Zoals met name het Europees Comité voor gegevensbescherming heeft verklaard: « *the EDPB stresses again* [EDPB-EDPS Joint Opinion 4/2022 and EPDB Statement 1/2024] *that encryption is* ***essential for ensuring the security and confidentiality of personal data and electronic communications****, as it provides strong technical safeguards against access to that information by anyone other than the user and the recipients chosen by him, including by the provider. In particular, in the context of interpersonal communications, genuine end-to-end encryption ('E2EE') covering the terminal devices and the data therein, with the decryption keys held solely by the users is a crucial*

[16] Zie https://docs.un.org/A/RES/79/243, laatstelijk geraadpleegd op 16/09/2025.

[17] Deze bepaling luidt als volgt:

"Elke staat die partij is, neemt de wettelijke en andere maatregelen die nodig zijn om zijn bevoegde autoriteiten te machtigen om elke persoon die kennis heeft van de werking van het betrokken informatie- en communicatiesysteem, het informatie- en telecommunicatienetwerk of de onderdelen daarvan, of van de maatregelen die worden toegepast om de daarin opgenomen elektronische gegevens te beschermen, te verplichten om, voor zover redelijk, alle informatie te verstrekken die nodig is om de in de paragraaf 1 tot en met 3 van dit artikel bedoelde maatregelen te kunnen toepassen." (vrije vertaling)

Zonder in detail te treden over deze bepalingen, verwijst punt 1. van hetzelfde artikel naar computeronderzoek, punt 2. naar de uitbreiding daarvan en punt 3. naar de inbeslagname van informaticasystemen en het kopiëren van elektronische gegevens.

[18] Zie ook advies nr. 69/2025 van 26 augustus 2025 met betrekking tot de "*Nationale Cybersecurity Strategie 3.0, 2026-2030" (CO-A-2025-108)*, punt 21.

tool for ensuring the confidentiality of electronic communications. ***Preventing the use of encryption or weakening the effectivity of the protection it provides, would have a severe impact on the respect for private life and confidentiality of users, on their freedom of expression as well as on innovation and the growth of the digital economy, which relies on the high level of trust and confidence that such technologies provide.*** »[19] (vetgedrukt door de Autoriteit)

26. Ten slotte verduidelijkte de aanvrager het volgende in zijn antwoorden op het derde verzoek om aanvullende informatie van de Autoriteit:

> "*De medewerking van de operator/verstrekker voor het opheffen van de eventueel toegepaste versleuteling zal alleen plaatsvinden als deze versleuteling door de verstrekker of de operator zelf is uitgevoerd (bijvoorbeeld: versleuteling van de verbindingen tussen de apparatuur van de verstrekker of de operator zelf).* ***De medewerking van de operator of verstrekker zal nooit worden gevraagd om end-to-end of op applicatieniveau versleutelde communicatie te ontsleutelen.*** *Het is bovendien duidelijk dat voor versleutelde communicatie de gegevens die na dubbele filtering beschikbaar zullen zijn voor de agenten van de ADIV, beperkt zullen blijven tot metagegevens. Als toegang tot de inhoud vereist is of als identificatie van het IP-adres noodzakelijk blijkt, zal in deze gevallen een beroep worden gedaan op andere methoden voor het verzamelen van gegevens die in de organieke wet worden beschreven.*" (vetgedrukt door de Autoriteit)

27. In deze omstandigheden stelt de Autoriteit allereerst vast dat **het dispositief van het ontwerp <u>geen verplichting bevat</u> voor operatoren en verstrekkers van elektronische communicatie <u>om mee te werken aan het ontcijferen</u>** van elektronische communicatie die uiteindelijk wordt onderschept.

28. Indien het de bedoeling van de auteur van het ontwerp is om in deze samenwerking te voorzien, **moet hij het <u>ontwerp aanpassen</u>, rekening houdend met de bovenstaande ontwikkelingen.** In dit verband moet in het ontwerp ten minste expliciet worden bepaald dat:

---

[19] EDPB, "Statement 5/2024 on the Recommendations of the Hight-Level Group on Access to Data for Effective Law Enforcement", vastgesteld op 4 november 2024, punt 3, beschikbaar op https://www.edpb.europa.eu/system/files/2024-11/edpb_statement_20241104_ontherecommendationsofthehlg_en.pdf, laatstelijk geraadpleegd op 30/07/2025. Recenter, zie ook EDPS, Opinion 23/2025 on the two Proposals for Council Decisions on the signing and conclusion of the United Nations Convention against Cybercrime, beschikbaar op https://www.edps.europa.eu/system/iles/2025-09/25-09-04_opinion_united_nations_convention_against_cybercrime_en.pdf, laatstelijk geraadpleegd op 20/10/2025, punt 48 :

"*In the digital age, technical solutions to secure and protect the confidentiality of electronic communications, including measures for encryption, are key to ensure the enjoyment of all fundamental rights* […]. *The EDPS therefore calls on Member States to carefully consider the potential impact, in particular on fundamental rights and cybersecurity, of any measures that might result in the weakening or degrading of encryption* […]. *In particular, Member States should abstain from imposing any obligations that would weaken data security for all users of an electronic communications service.*"

- Ten eerste de medewerking aan het ontcijferen van de betrokken elektronische communicatie **alleen betrekking heeft op de technische versleutelingsoplossing die door de betrokken operator of verstrekker van elektronische-communicatiediensten zelf wordt toegepast;**

- Ten tweede deze medewerking **niet mag leiden tot een vermindering van de kwaliteit van de door deze operator of verstrekker gekozen technische versleutelingsoplossing voor andere gebruikers van wie de elektronische communicatie niet mag worden onderschept.** Met andere woorden, de verplichting tot medewerking van de betrokken dienstaanbieders mag geen invloed hebben op het niveau en de kwaliteit van de technische versleutelingsoplossing die zij aanbieden aan gebruikers van wie de communicatie niet mag worden onderschept. **Als er geen oplossing beschikbaar is gezien de versleutelingstechniek die door de operator of de verstrekker van elektronische-communicatiediensten is gekozen, kan de medewerking dus niet plaatsvinden;**

- En ten derde, zoals de aanvrager heeft aangegeven, **de medewerking van de operator of verstrekker niet kan worden gevraagd om end-to-end of op applicatieniveau versleutelde communicatie te ontsleutelen.**

29. Dit gezegd zijnde, moet deze vraagstelling in aanmerking worden genomen in de algemene aanbeveling van de Autoriteit om **een geactualiseerd parlementair debat te voeren over de artikelen 44 en 44/5 van de I&V-wet[20].**

II.2.4 Interacties met het internationaal publiekrecht

30. In twee van zijn adviezen stelt de Raad van State een internationaalrechtelijk probleem aan de orde dat verband houdt met de I&V-wet in de context van het onderhavige advies[21]. De Autoriteit heeft de aanvrager gevraagd hoe dit probleem wordt opgelost wanneer de gevraagde medewerking betrekking heeft op elektronische communicatie die uitsluitend buiten het rechtsgebied van België plaatsvindt[22]. De aanvrager antwoordde het volgende:

[20] Zie punt 69.

[21] Zie met name advies van de Raad van State nr. 32.623/4 van 28 januari 2002, *met betrekking tot een voorontwerp van wet 'tot wijziging van artikel 44 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten',* pp. 3-7.

[22] Bijvoorbeeld een e-mailwisseling via Hotmail over personen A en B die geen Belgische ingezetenen zijn en geen gebruik maken van Hotmail vanuit België, maar wel betrokken zijn bij de activiteiten van een organisatie die op de lijst staat.

"*Hoewel de instellingen/organisaties op de lijsten niet automatisch Belgische ingezetenen en/of vanuit België gebruikte diensten betreffen, houden de activiteiten van deze instellingen/organisaties rechtstreeks verband met de belangen die door de ADIV worden beschermd en die in zijn opdrachten in artikel 11, § 1, van de organieke wet worden uiteengezet.*

Bovendien bevat het internationaal recht tot op heden geen duidelijke bepaling die de interceptie van elektronische communicatie vanaf het grondgebied van een staat verbiedt en die is gericht op communicatie tussen personen buiten zijn rechtsgebied, met name in het kader van inlichtingenoperaties in verband met de nationale veiligheid.

Hoewel bepaalde algemene beginselen van het internationaal recht kunnen worden ingeroepen (met name de eerbiediging van de soevereiniteit van staten, de niet-inmenging in binnenlandse aangelegenheden of de bescherming van de persoonlijke levenssfeer), is de concrete toepassing ervan op cyberspace, en met name op extraterritoriale intercepties voor inlichtingendoeleinden, nog steeds voorwerp van discussie op internationaal niveau. Op dit moment bestaat er geen juridische consensus dat dit soort interceptie volgens het internationaal recht verboden is."

31. De Autoriteit neemt akte van deze uitleg. **Het is aan de Raad van State om zich hierover uit te spreken, en op basis van diens conclusies is het aan de auteur van het ontwerp om hieruit consequenties te trekken met betrekking tot de rechtmatigheid van de beoogde gegevensverwerkingen.** De beoordeling van het ontwerp in het licht van het internationaal publiekrecht is des te belangrijker omdat het toepassingsgebied ervan zo breed is.

II.3. Specifiek controlesysteem voor interceptie en extraneïteit van de betreffende situatie

32. De Autoriteit heeft in de memorie van toelichting bij de wet van 2017 gezocht naar **redenen die aanleiding zouden kunnen geven tot de invoering van een ad hoc en minder streng wettelijk stelsel voor de controle** van de ADIV op de interceptie van **in het buitenland verzonden of ontvangen** elektronische communicatie.

33. Het hoeft misschien niet meer te worden benadrukt[23], maar de Autoriteit wil er toch op wijzen dat overeenkomstig artikel 1 van het EVRM de **in het EVRM vastgelegde rechten** niet alleen van toepassing zijn op het Belgisch grondgebied. Ze zijn namelijk **van toepassing op iedereen** die onder de Belgische jurisdictie valt, dat wil zeggen onder Belgische rechts**bevoegdheid**[24].

34. De memorie van toelichting vermeldt het volgende met betrekking tot het binnendringen in informaticasystemen[25]: "*De thans vastgelegde procedures voor de toepassing van een uitzonderlijke methode bij operaties in het buitenland zijn niet altijd toepasbaar, aangezien de inlichtingenbehoefte (art. 11, § 1, 1°) en de behoefte aan veiligheid (art. 11, § 1, 2°), nog meer in het buitenland, onmiddellijk zijn en niet altijd, zelfs enkele uren, de tijd die nodig is voor het volgen van de hoogdringendheidsprocedure, kunnen wachten, aangezien de dreiging niet potentieel, maar concreet en imminent is. De tijdsverschillen vergemakkelijken de zaken niet en, bovenal, zijn de communicaties naar België niet altijd mogelijk en zelfs niet altijd beveiligd. Bovendien is het soms zeer moeilijk om een nauwkeurig doel te identificeren.*"[26]

35. Meer in het algemeen, en ditmaal **met betrekking tot de prerogatieven van de ADIV in het buitenland, vermeldt de memorie van toelichting bij de wet van 2017 ook het volgende**[27]: "*In het kader van bepaalde operaties is het absoluut noodzakelijk om informatie te verzamelen, maar is het* ***de ADIV om verschillende redenen onmogelijk de vastgelegde procedure voor de aanwending van specifieke en uitzonderlijke methoden te volgen: in het buitenland, tijdsverschil, hoogdringendheid, geen enkel beveiligd communicatiemiddel, onmogelijkheid om zich te richten op een specifieke persoon of gebeurtenis****... Bijgevolg zouden* ***bepaalde wijzen van informatiegaring flexibeler moeten worden*** *terwijl de controle op die informatiegaring behouden blijft."*[28] (vetgedrukt door de Autoriteit)

---

[23] De Raad van State heeft al lang geleden op dit punt gewezen, zie advies va de Raad van State nr. 32.623/4 van 28 januari 2002, *met betrekking tot een voorontwerp van wet 'tot wijziging van artikel 44 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten",* p. 8.

[24] Zie Europees Hof voor de Rechten van de Mens, "Fiche thématique — Juridiction extraterritoriale des Etats parties", juli 2018, beschikbaar via https://www.echr.coe.int/documents/d/echr/fs_extra-territorial_jurisdiction_fra, laatstelijk geraadpleegd op 16/09/2025.

[25] Gevraagd naar deze kwestie, wees de aanvrager de Autoriteit erop dat deze passage wel degelijk betrekking had op het binnendringen in informaticasystemen en niet op de interceptie van elektronische communicatie.

[26] *Parl. St.*, Kamer van volksvertegenwoordigers, nr. 54-2043/001, p. 84.

[27] *Parl. St.*, Kamer van volksvertegenwoordigers, nr. 54-2043/001, p. 7.

[28] De memorie van toelichting vervolgt:

Thans kan de ADIV in het buitenland uitgezonden communicatie intercepteren volgens een jaarlijks afluisterplan dat een lijst behelst van de organisaties en instellingen die het onderwerp zullen zijn van intercepties en dat is goedgekeurd door de minister van Defensie en overgezonden aan het Comité I.

De aanvrager stelt voor dezelfde procedure te gebruiken voor de intrusie in een buitenlands informaticasysteem (uitzonderlijke methode) en de opname van beelden (specifieke of uitzonderlijke methode naargelang de plaats) in het buitenland, op grond van een jaarplan intrusie en beeldopname.

Daardoor zal de ADIV bijvoorbeeld onmiddellijk kunnen binnendringen in de gsm van een kamikaze die zich in het buitenland bevindt, om na te gaan of hij al dan niet van plan is om een tuig te laten ontploffen, mits deze kamikaze lid is van een in het jaarplan bedoelde organisatie.

36. **De situatie waarop het ontwerp betrekking heeft, lijkt echter anders te zijn**, aangezien zij schriftelijke communicatie tussen de ADIV en de verstrekkers van elektronische-communicatiediensten en operatoren vereist, en zelfs de installatie van apparatuur "bij" deze aanbieders. Concreet zullen intercepties in België plaatsvinden wanneer de operator of de verstrekker zich in België bevindt, maar ook wanneer er in België gebruik wordt gemaakt van technische infrastructuur[29].

37. In deze context is het overigens **moeilijk om de territoriale reikwijdte van artikel 44 duidelijk te bepalen**. De Autoriteit heeft de aanvrager om **opheldering gevraagd over de vraag welk element van extraneïteit is vereist vanuit het oogpunt van de activiteiten van de ADIV, opdat de artikelen 44 en 44/5 van toepassing zouden zijn**. Bij lezing van deze bepalingen lijkt het niet noodzakelijk dat een agent van de ADIV fysiek aanwezig is in het geografische gebied waar de betrokken organisatie of instelling zich bevindt, opdat deze bepalingen van toepassing kunnen zijn. Kan de ADIV de elektronische communicatie van en naar een ander land C verkrijgen wanneer een organisatie of instelling van belang zich daar bevindt, ondanks het feit dat de ADIV ter plaatse geen fysieke activiteiten uitvoert, voor zover de betrokken organisatie of instelling betrokken is bij een dreiging als bedoeld in artikel 11, § 1, 1° tot 3° en 5° van de I&V-wet? De aanvrager antwoordde het volgende:

> "***Inderdaad. De juridische elementen die de toepassing van de artikelen 44 en 44/5 mogelijk maken, zijn het feit dat de communicatie in het buitenland wordt verzonden of ontvangen*** *en dat deze afkomstig is van instellingen/organisaties die zijn opgenomen in de lijsten bedoeld in artikel 44/3*." (vetgedrukt door de Autoriteit)
>
> "*Dat is de bedoeling, maar om precies te zijn: de ADIV zal de communicatie kunnen verkrijgen als de betrokken organisatie of instelling wel degelijk voorkomt op de lijsten bedoeld in artikel 44/3 van de organieke wet. Deze lijsten worden jaarlijks goedgekeurd volgens de procedure beschreven in het eerdergenoemde artikel 44/3 en vermelden voor elke organisatie of instelling de reden waarom zij het voorwerp zal uitmaken van een interceptie in verband met de in artikel 11, § 1, 1° tot 3° en 5°, bedoelde opdrachten."*

38. **Ten aanzien van deze elementen vraagt de Autoriteit zich af hoe** in het kader van het ontwerp **kan worden gerechtvaardigd** dat de door de ADIV uitgevoerde intercepties **niet onderworpen zijn aan de natuurlijke waarborgen die van toepassing zijn op uitzonderlijke methoden voor het verzamelen van inlichtingen** (zie de methode van artikel 18/17 van de I&V-wet, die met

[29] Zie het antwoord van de aanvrager, aangehaald in punt 16 ("*De communicatie die het voorwerp uitmaakt van de samenwerking tussen de verstrekker of operator en de ADIV zou in dat geval worden doorgestuurd naar de installaties in België*").

name een voorafgaande toestemming van de BIM-commissie vereist). De Autoriteit heeft de aanvrager hiernaar gevraagd en deze verstrekte de volgende aanvullende informatie:

> "Alvorens deze vraag te beantwoorden, is het belangrijk op te merken dat het doel van het ontwerp van koninklijk besluit erin bestaat de modaliteiten van de medewerking van de operator/verstrekker vast te leggen. *Het ontwerp van koninklijk besluit legt geen nieuwe methode voor de interceptie van gegevens vast, aangezien dit reeds mogelijk is en geregeld wordt door de artikelen 44 en 44/3 van de wet van 30 november 1998.* ***De voorbeelden die in de memorie van toelichting*** *bij de wet van 2017 worden genoemd,* ***zijn niet uitputtend en hebben niet allemaal betrekking op artikel 44. Andere situaties, die op afstand door de ADIV worden gevolgd, kunnen een soepeler kader*** *rechtvaardigen dan het kader van de uitzonderlijke methoden. Het is namelijk* ***niet altijd mogelijk om vooraf de (potentiële) ernst van een buitenlandse dreiging in te schatten, noch om vooraf te bepalen of aan de strenge wettelijke voorwaarden voor het gebruik van een uitzonderlijke methode is voldaan.*** Kortom, het genoemde hoofdstuk V is opgesteld om tegemoet te komen aan de specifieke behoeften van de inlichtingendienst in het buitenland, **met name in situaties waarin de toepassing van de regeling inzake uitzonderlijke methoden (en met name de voorafgaande controle door de BIM-commissie) operationeel niet haalbaar zou zijn, ongeacht of de ADIV daadwerkelijk ter plaatse aanwezig is.**" (vetgedrukt door de Autoriteit)

39. **De Autoriteit neemt akte van deze uitleg, maar <u>is echter niet volledig overtuigd</u>.** De door de aanvrager gegeven motivering maakt het immers niet mogelijk om concreet te begrijpen waarom het controlesysteem voor uitzonderlijke methoden voor het verzamelen van gegevens niet geschikt is in de situaties waarop het ontwerp betrekking heeft. **Gezien de uitgebreide ervaring van het Comité I en zijn betere bekendheid met deze materie, <u>kiest de Autoriteit ervoor zich te baseren op het standpunt dat het Comité zou innemen over de eventuele noodzaak om een ad-hoccontrole in te voeren en te regelen</u>** (los van de normale controle van uitzonderlijke inlichtingenmethoden), en is zij bovendien van mening **dat de motivering van het huidige wettelijk kader <u>absoluut moet worden onderbouwd</u>**. **In de huidige situatie beschikt de Autoriteit niet over de nodige informatie om zich te kunnen uitspreken.**

40. In elk geval, indien het Comité I van mening is dat de betrokken intercepties en samenwerkingen geen minder beschermende ad-hoccontrole rechtvaardigen, moeten conclusies worden getrokken over de rechtmatigheid van de verwerkingen die aan operatoren en verstrekkers van elektronische-communicatiediensten worden opgelegd.

41. Dit doet geen afbreuk aan het feit dat het **wel degelijk onder de bevoegdheid van de Autoriteit valt om te beoordelen of de vereiste medewerking van operatoren en verstrekkers van elektronische-communicatiediensten in het kader van deze dienstverleningsactiviteiten in overeenstemming is met het toepasselijke recht[30]** (opmerking: de situatie waarin de ADIV zelf zou optreden zonder medeweten en zonder medewerking van een operator of verstrekker van elektronische communicatie is juridisch gezien een heel andere situatie[31]). Met andere woorden, de Autoriteit moet zich uitspreken over het mogelijk ontbreken van passende waarborgen in deze context.

42. In dit kader heeft zij de aanvrager gevraagd naar de rechtvaardiging van artikel 44 van de I&V-wet in het licht van de **rechtspraak van het HvJ-EU op het gebied van afwijkingen van de vertrouwelijkheid van elektronische communicatie**[32] (met name in het kader van de ad-hoccontrole mag het Comité I geen toegang tot de betreffende gegevens verlenen, en bovendien voorzien de lijsten meer in een algemeen programma voor interceptie dan in een concrete lijst van te onderscheppen communicatie). De aanvrager antwoordde het volgende:

> "*De enige communicatie die kan worden onderschept, is die **met betrekking tot de instellingen/organisaties van de lijsten** bedoeld in artikel 44/3 van de organieke wet. De lijsten voorzien dus niet in een algemeen programma voor interceptie, maar wel in een **gericht overzicht van organisaties en instellingen.***
> *Overeenkomstig het bovengenoemde artikel 44/3 **heeft het Comité I controle vóór**, tijdens en na de intercepties die worden uitgevoerd.*
> *Wat betreft de controle "vóór" de intercepties, **worden de lijsten van artikel 44/3 goedgekeurd door de minister van Defensie en ook naar het Comité I gestuurd**. In zijn rol als toezichthoudende autoriteit op de activiteiten van de ADIV kan het Comité I te allen*

---

[30] "*Volgens vaste rechtspraak van het Hof staat het immers weliswaar aan de lidstaten om hun wezenlijke veiligheidsbelangen te definiëren en om passende maatregelen te nemen teneinde hun binnenlandse en buitenlandse veiligheid te verzekeren, maar kan het enkele feit dat een nationale maatregel is genomen met het oog op de bescherming van de nationale veiligheid, niet ertoe leiden dat het Unierecht niet van toepassing is en dat de lidstaten worden ontheven van de verplichting om dit recht te eerbiedigen [zie in die zin arresten van 4 juni 2013, ZZ, C-300/11, EU:C:2013:363, punt 38 en aldaar aangehaalde rechtspraak; 20 maart 2018, Commissie/Oostenrijk (Staatsdrukkerij), C-187/16, EU:C:2018:194, punten 75 en 76, en 2 april 2020, Commissie/Polen, Hongarije en Tsjechië (Tijdelijk herplaatsingsmechanisme voor aanvragers van internationale bescherming), C-715/17, C-718/17 en C-719/17, EU:C:2020:257, punten 143 en 170]"* HvJ-EU Grote kamer), arrest van 6 oktober 2020 Google Spain, zaak C-623/17, punt 44. Zie ook HvJ-EU Grote kamer), arrest van 6 oktober 2020, La Quadrature du Net, gevoegde zaken C-511/18, C-512/18 en C-520/18, punten 87-104.

[31] Zie ook punt 70.

[32] In dit verband, zie de volgende arresten: HvJ-EU (Grote kamer), arrest van 20 september 2022, Bundesrepublic Deutschland t/ SpaceNet AG, Telekom Deutschland GmbH, gevoegde zaken C-793/19 en C-794/19; HvJ-EU (Grote kamer), arrest van 5 april 2022, G.D. t. Commissioner of the Garda Siochána e.a., zaak C-140/20; HvJ-EU (Grote kamer), arrest van 6 oktober 2020, La Quadrature du Net, gevoegde zakenC-511/18, C-512/18 en C-520/18; HvJ-EU (Grote kamer), arrest van 21 december 2016, Tele2 Sverige, gevoegde zaken C-203/15 en C-698/15; HvJ-EU (Grote Kamer), arrest van 8 april 2014, Digital Rights Ireland, gevoegde zaken C-293/12 en C-594/12.

Zie ook HvJ-EU (Grote kamer), arrest van 6 oktober 2020, Privacy International, zaak. C-623/17, met name de punten nrs. 61 en 76 (en de aangehaalde rechtspraak in de punten 65, 67-68); HvJ-EU (Derde kamer), arrest van 16 februari 2023, Hya, IP, DD, ZI, en SS, zaak C-349/21. 162/22

tijde bezwaar maken tegen deze lijsten, de intercepties stopzetten en de vernietiging van de verzamelde gegevens gelasten.

Het Comité I beschikt dus wel degelijk over een voorafgaande controle op dit gebied, die zowel voortvloeit uit de in artikel 44/3 beschreven controlemodaliteiten als uit de algemene bevoegdheden van het Comité als controle-instantie van de ADIV." (vetgedrukt door de Autoriteit)

43. De Autoriteit neemt akte van deze uitleg. Onverminderd de overwegingen in punt 39, en met name gezien de aanzienlijke inmenging die de artikelen 44 en 44/5 van de I&V-wet met zich meebrengen, **ziet de Autoriteit niet op welke basis**, in het licht van de bovengenoemde Europese rechtspraak[33], **het gerechtvaardigd zou zijn om de ADIV vrij te stellen van een voorafgaande beslissing (toestemming) van de BIM-commissie (of het vast Comité I), behalve in dringende gevallen**, zoals bepaald in het kader van het gebruik van uitzonderlijke methoden voor het verzamelen van gegevens.

44. In een situatie zoals die welke in dit advies aan de orde is (namelijk de interceptie van elektronische communicatie door een inlichtingendienst), **zijn dergelijke procedurele waarborgen des te belangrijker** omdat het niet altijd mogelijk is om in de toepasselijke wetgeving precies aan te geven welke categorieën van gegevens zullen worden verwerkt. De Autoriteit heeft reeds benadrukt dat, wat strafrechtelijke autoriteiten en controle-/inspectiediensten betreft, de essentiële elementen van de voorgenomen verwerking van persoonsgegevens (waaronder de categorieën van gegevens) en de evenredigheid daarvan over het algemeen zullen voortvloeien uit een gecombineerde lezing van de regels die zij handhaven en de bevoegdheden die hun bij wet zijn toegekend, met inbegrip van de beperkingen en procedurele waarborgen die daarin zijn vastgelegd[34].

45. Bovendien is de Autoriteit van mening dat de in het ontwerp beoogde regeling **in werkelijkheid**, op het niveau van de betrokken operatoren of verstrekkers van elektronische-communicatiediensten en **ten aanzien van de gebruikers die betrokken zijn** bij de ingevoerde selectie van datastromen, **leidt tot een besluitvorming die uitsluitend is gebaseerd op een geautomatiseerde gegevensverwerking waarbij profilering wordt toegepast, die voor hen rechtsgevolgen heeft en hen aanzienlijk treft**, aangezien hun communicatieverkeer wordt doorgegeven aan een inlichtingendienst voor verwerking door die dienst, met name in een normatieve context waarin hun rechten overeenkomstig het nationale recht zijn beperkt. Wat dit betreft, vereist artikel **22 van de AVG** dat

[33] Zie voetnoot 32.

[34] Zie advies nr. 129/2022 van 1 juli 2022 *betreffende de artikelen 2 en 7 tot en met 47 van een ontwerp van wet houdende diverse bepalingen inzake Economie* (CO-A-2022-110); en advies nr. 252/2022 van 1 december 2022 *met betrekking tot een voorontwerp van wet tot hervorming van boek II van het Strafwetboek (CO-A-2022-281)*, punt 9.

passende maatregelen worden getroffen om de rechten en vrijheden en de gerechtvaardigde belangen van de betrokkenen te beschermen.

46. Ten slotte moet met betrekking tot **artikel 19 van het ontwerp**, dat een **controleopdracht toekent aan het Comité I**, in dit advies worden verwezen naar **punt 13 van het advies van het Comité I**, waarin met name wordt gesteld:

> "*Artikel 19 belast het Comité met een controleopdracht op de samenwerking tussen de ADIV en de betrokken netwerkoperator of dienstverstrekker. Deze bijzondere controle is drieledig. 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[***[35]***], indachtig de hoge mate van techniciteit van de samenwerking tussen de ADIV en de betrokken netwerkoperator of dienstenverstrekker, niet realistisch 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 i****s 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.*" (vetgedrukt door de Autoriteit)

47. De Autoriteit sluit zich aan bij het standpunt van het Comité I. **Als geen rekening wordt gehouden met het advies van het Comité I op dit punt, loopt de auteur van het ontwerp het risico**

[35] De termijn waarin het ontwerp voorziet, is meer bepaald "*veertien werkdagen vanaf de verzending van het verzoek*". Dit verandert niets aan het commentaar van het Comité I.

een controle in te voeren die slechts schijn is en waarvan de doeltreffendheid twijfelachtig is. Dit is des te belangrijker gezien het vertrouwelijke karakter van de activiteiten van de ADIV, die alleen door het Comité I mogen worden gedeeld.

II.4 De door het ontwerp ingevoerde regeling, op basis van de I&V-wet

II.4.1 Het ontwerp en de I&V-wet

48. Allereerst merkt de Autoriteit op dat de betrokken operator of verstrekker van elektronische-communicatiediensten **verplicht is een samenwerkingsakkoord te sluiten met de ADIV, en dat bij gebrek aan een akkoord twee ministers de voorwaarden voor de beoogde samenwerking kunnen vaststellen.** Dit samenwerkingsakkoord "*vult de algemene modaliteiten voor samenwerking aan die in de artikelen 11 tot en met 17 worden beschreven en omvat ten minste de gedetailleerde technische, organisatorische en financiële bepalingen*."[36] De betrokken dienstenaanbieder en de ADIV hebben negen maanden de tijd om deze overeenkomst te sluiten. Bij het ontbreken van een samenwerkingsakkoord binnen de gestelde termijn, en op verzoek van een van de partijen, "*bepalen de minister van Defensie en de minister van Telecommunicatie gezamenlijk, binnen een termijn van 3 maanden [...] bij ministerieel besluit de modaliteiten van de hierboven bedoelde samenwerking*."[37]

49. **Artikel 14 van het ontwerp**, dat de kern vormt van de beoogde regeling, luidt als volgt:

> "***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 i****n 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.*" (vetgedrukt en onderstreept door de Autoriteit)

[36] Artikel 9, § 1, van het ontwerp.

[37] Artikel C.VI.24, § 2 van het ontwerp.

50. Deze bepaling voorziet in de invoering van **twee technische oplossingen**, die **onder verschillende verantwoordelijkheden lijken te vallen (operator of verstrekker/ADIV).** De operator of verstrekker is verantwoordelijk voor het installeren van "***een technisch systeem***" op zijn infrastructuur, onder zijn verantwoordelijkheid, voor het selecteren van elektronische communicatie en het doorsturen daarvan naar "***de apparatuur van de ADIV die is geplaatst bij de***" betrokken verstrekker of operator, die onder de exclusieve verantwoordelijkheid van de ADIV valt (toepassing van **filtering** om de elektronische communicatiegegevens te identificeren die concreet nodig zijn voor de uitvoering van de betreffende opdracht van de ADIV).

51. Deze regeling roept echter verschillende vragen op, die aan de aanvrager zijn voorgelegd. **De I&V-wet en het ontwerp bepalen namelijk niet op basis van welke concrete gegevens/criteria de betrokken elektronische communicatie op het niveau van de operator of de verstrekker van elektronische-communicatiediensten (**d.w.z. op het niveau van het **"technische systeem") kan worden gefilterd.** De I&V-wet beperkt zich tot het opstellen van een jaarlijkse lijst met organisaties of instellingen die worden onderworpen aan intercepties, de reden waarom dergelijke intercepties mogen plaatsvinden en de duur ervan. Artikel 14, tweede lid, van het ontwerp vermeldt als selectiecriterium alleen de betreffende "*geografische gebieden waar zich instellingen en organisaties bevinden die deel uitmaken van de lijsten*".

II.4.2 Aanvullende informatie verstrekt door de aanvrager

52. De Autoriteit heeft de aanvrager talrijke vragen gesteld over de betreffende filtering en de gegevens/criteria die in dit verband aan de operatoren worden meegedeeld[38], en over de actualisering van de filtering, rekening houdend met het feit dat de "afluisterlijsten" op jaarbasis worden opgesteld[39]. Na een eerste reeks antwoorden heeft zij hem opnieuw ondervraagd om duidelijk te kunnen vaststellen wat de *input* (vanuit het systeem van de operator/verstrekker) en *output* (naar de apparatuur van de

[38] De Autoriteit heeft de aanvrager gevraagd: een fictief illustratief uittreksel van een lijst te verstrekken; aan te geven op basis van welke gegevens de betrokken operator of verstrekker zal worden verplicht de communicatie in kwestie te selecteren (welke soorten filters (filtergegevens) aan de operator worden meegedeeld) (Als het bijvoorbeeld gaat om de interceptie van telefoongesprekken, worden dan de telefoonnummers doorgegeven die vermoedelijk door de betrokken instellingen of organisaties worden gebruikt? Als het gaat om de interceptie van IP-verkeer, worden dan de IP-adressen meegedeeld die vermoedelijk door deze organisaties worden gebruikt? Wat gebeurt er in het geval van de interceptie van e-mails of communicatie via een mobiele applicatie?); te verduidelijken of het gaat om de interceptie van al het verkeer van en naar een land, en hoe ten aanzien van de operator wordt vastgesteld dat de betrokken communicatie daadwerkelijk afkomstig is uit het beperkte geografische gebied waarbinnen de betrokken instelling of organisatie actief is (wordt in dit verband rekening gehouden met het gebruik van tussenpersonen (proxyservers) die verhinderen dat een communicatie aan haar werkelijke geografische oorsprong kan worden gekoppeld?).

[39] De I&V-wet en het ontwerp voorzien in een jaarlijkse samenwerking (de lijsten zijn jaarlijks) tussen de betrokken operatoren en verstrekkers. Met andere woorden, in principe (dat wil zeggen, behalve in het geval van een dringende en onvoorziene, noodzakelijke interceptie) wordt aan deze verstrekkers voor het betreffende jaar slechts één lijst met "filters" of "filtergegevens" verstrekt. De Autoriteit heeft de aanvrager gevraagd hoe deze informatie (deze filters) met betrekking tot deze verstrekkers wordt bijgewerkt, aangezien in de praktijk de abonnementen op de verschillende elektronische-communicatiediensten (internet, 5G, e-mail, chats, applicaties, enz.) in de loop van de tijd kunnen veranderen.

ADIV) was, in termen van elektronische communicatiegegevens, van het "bij" de operator of verstrekker van elektronische-communicatiediensten geplaatste "*technische systeem*" (zie punt 51). Ten slotte heeft de Autoriteit, na de aanstelling van een externe deskundige, de aanvrager een derde verzoek om aanvullende informatie gestuurd.

53. De volgende elementen zijn met name door de aanvrager meegedeeld (opmerking: in het onderhavige advies zijn de niet geciteerde passages uit de door de aanvrager verstrekte antwoorden weggelaten omdat ze niet relevant zijn ten aanzien van de gestelde vraag):

> Wat betreft de **rol van de operator/verstrekker met betrekking tot de filtering** en de filters die aan hem zouden worden meegedeeld:
>
> "*[...] De* ***verantwoordelijkheid voor de filtering ligt uitsluitend bij de ADIV****. Het ontwerp van koninklijk besluit zou op dit punt eventueel verder kunnen worden verduidelijkt (met name in het verslag aan de Koning).*"(vetgedrukt en onderstreept door de Autoriteit)
>
> "***Deze elementen worden uitsluitend bepaald en uitgevoerd door de ADIV****, in het kader van de controle door het Comité I zoals bepaald in de organieke wet.* ***De operator heeft geen zicht op de onderschepte gegevens, noch heeft hij enige controle of verantwoordelijkheid in dit verband.*** *Als dit punt niet duidelijk is in het huidige ontwerp van koninklijk besluit, kan het in toekomstige wijzigingen worden verduidelijkt.*
>
> ***De medewerking van de operator*** *is voornamelijk* ***gericht op het implementeren van een technische oplossing waarmee de gegevens kunnen worden gedupliceerd naar de apparatuur van de ADIV, die zodanig zal worden geconfigureerd dat alleen communicatie wordt onderschept die in het buitenland wordt verzonden of ontvangen door de in artikel 44/3 genoemde organisaties/instellingen.****"* (vetgedrukt en onderstreept door de Autoriteit)
>
> Wat betreft de **lijsten van organisaties/instellingen**:
>
> "[...] *De lijst voor interceptie zou bijvoorbeeld de inlichtingen- en veiligheidsdiensten van het land REDLAND kunnen bevatten; de Algemene Administratie van Militaire Inlichtingen van REDLAND zou dus op de lijst kunnen staan.* […]"
>
> Wat betreft de vraag of het gaat om de interceptie van al het **verkeer van en naar een land**, verwees de aanvrager naar een eerder antwoord in dit punt en voegde hij het volgende toe:

"*Zie vorig antwoord: de controle op dit gebied wordt uitgevoerd door de entiteit die belast is met de controle van de activiteiten van de ADIV, namelijk het Comité I, en volgens het daarvoor vastgestelde wettelijk kader (met name de organieke wet, de wet op de persoonlijke levenssfeer en de specifieke wet voor het Comité I van 18 juli 1991). Ter informatie vindt u hieronder enkele* ***voorbeelden van mogelijke filterparameters*** *(niet-uitputtende lijst), afhankelijk van het type verstrekker en het type samenwerking dat wordt beoogd:*

- *landcodes of regionale prefixen (telefoonoperator),*
- *IP-adressen of Border Gateway Protocol-routeringsinformatie (dienstverstrekker type ISP),*
- *door uitsluitend te richten op specifieke interconnecties die van belang zijn (dienstverstrekker van optische verbindingen).*

De problematiek rond het gebruik van VPN's en andere technische oplossingen om de exacte locatie van de bron van een IP-communicatie te verbergen, is welbekend bij de ADIV, maar vormt geen voldoende beperking om niet de medewerking van operatoren of verstrekkers te vragen, gelet op het feit dat dit slechts van toepassing is op bepaalde vormen van samenwerking en op een beperkt aantal organisaties." (vetgedrukt door de Autoriteit)

Wat betreft de samenwerking op jaarbasis via een algemeen verzoek met een lijst van operatoren/verstrekkers **en de actualisering van deze lijsten**:

"[...] *Meer bepaald* ***bestaat de medewerking van de operator of verstrekker*** *niet in een actieve verwerking of analyse van de communicatie, maar in* ***de invoering van een technisch mechanisme waarmee bepaalde gegevensstromen*** *(in het buitenland verzonden of ontvangen elektronische communicatie)* ***kunnen worden gedupliceerd naar de beveiligde apparatuur van de ADIV die in zijn infrastructuur is geïnstalleerd****.*
Deze apparatuur wordt volledig geconfigureerd door de ADIV, die als enige verantwoordelijk is voor de implementatie van de filtering *in overeenstemming met de lijst van doelwitten zoals bepaald in artikel 44/3.* ***De operator/verstrekker heeft geen*** *toegang tot de onderschepte gegevens en heeft geen recht of plicht om de inhoud of de reikwijdte van de interceptie te controleren. De rol van de operator is dus strikt passief en technisch.*
Dit onderscheid is essentieel in het licht van de rechtspraak van het HvJ-EU, met name in het arrest Privacy International (C-623/17), *dat lidstaten verbiedt om operatoren een algemene en ongedifferentieerde verplichting tot het bewaren of doorgeven van elektronische communicatiegegevens op te leggen. Het ontwerp van koninklijk besluit beantwoordt aan deze verplichting, aangezien het niet voorziet in een massale en willekeurige verzameling van gege-*

vens, maar wel in een gerichte interceptie, die onderworpen is aan een strikt wettelijk, administratief en gerechtelijk kader en gecontroleerd wordt door het Comité I, overeenkomstig de vereisten van de organieke wet.
Indien het nodig is om dit punt verder te verduidelijken in de tekst van het koninklijk besluit of in het verslag aan de Koning, kan dit worden overwogen in toekomstige wijzigingen van het ontwerp in kwestie."
"Het bijwerken en configureren van de filters valt onder de verantwoordelijkheid van de ADIV. Dit zou in het ontwerp van koninklijk besluit verder kunnen worden toegelicht." (vetgedrukt door de Autoriteit)

54. In verband met de tweede reeks vragen die aan de aanvrager werden gesteld, en de in deze context verstrekte antwoorden:

Wat betreft de **gegevens waartoe het door de operator/verstrekker opgezette technische systeem toegang heeft**[40]:

"*Het door de operator/verstrekker opgezette "technische systeem" heeft tot doel* ***alle elektronische communicatie te dupliceren die specifiek is voor de dienst waarop de samenwerking betrekking heeft (bijvoorbeeld specifieke glasvezel, specifieke verbinding, enz.).***
[...] Deze samenwerking ***zal echter al specifiek gericht zijn op bepaalde soorten communicatie*** *(het voorwerp van de samenwerking zou bijvoorbeeld alleen betrekking kunnen hebben op één enkele glasvezel waarvan de herkomst of bestemming (in het buitenland) van specifiek belang is voor de uitvoering van de bovengenoemde opdrachten van de ADIV).* […]".

Over de ***input*** **die wordt ontvangen door het filtersysteem dat gebruikt wordt op de infrastructuur van de ADIV**[41]:

"*Om problemen met het bewaren, opslaan en vernietigen van gegevens bij de verstrekker/operator te voorkomen,* ***gebeurt de verzending in één keer en betreft deze alle***

[40] Klopt het dat het door de operator/verstrekker opgezette "technische systeem" toegang heeft tot alle gegevens (metagegevens en inhoud) met betrekking tot alle elektronische communicatie die via de betreffende dienst verloopt? Zo nee, wat is de situatie dan?

[41] Wordt de filtering die de ADIV op zijn apparatuur (zijn infrastructuur) uitvoert, gevoed met gegevens van alle elektronische communicatie die via de diensten van de operator/verstrekker verloopt? Zo nee, wat is de situatie dan? (Bijvoorbeeld: werkt het systeem in twee stappen, (1) verzending van alle metagegevens, (2) vervolgens verzending van de inhoudsgegevens na een eerste filtering op basis van de metagegevens; andere?).

elektronische communicatiegegevens ***die specifiek via een verzoek zijn opgevraagd*** *en in het samenwerkingsakkoord zijn vermeld.* ***Deze gegevens worden vervolgens in twee fasen gefilterd (PASS / DISCARD)****, op basis van de lijsten bedoeld in artikel 44/3 van de organieke wet. Een* ***eerste****,* ***grovere en niet-geclassificeerde filtering*** ***vindt plaats bij de verstrekker (soft filtering) en een tweede****,* ***nog specifiekere en geclassificeerde filtering*** ***vindt plaats binnen de infrastructuur van de ADIV.*** *Na deze tweede filtering wordt een (menselijke) relevantiebeoordeling uitgevoerd en worden alleen de gegevens die als relevant worden beschouwd, bewaard.*" (vetgedrukt en onderstreept door de Autoriteit)

Wat betreft de **configuratie van de technische systemen** die door de operator/verstrekker zijn geïnstalleerd en wat betreft **de aard ervan[42]:**

"*De technische systemen die door de verstrekker/operator zijn opgezet,* ***vereisen in principe geen specifieke configuratie****. De* ***precieze locatie*** *van deze "technische systemen"* ***binnen de architectuur*** *van de verstrekker of operator moet in samenwerking tussen de ADIV en de dienstverstrekker of operator worden bepaald, zodat uitsluitend de communicatie waarop het verzoek betrekking heeft, wordt aangepakt."*

*"De keuze van het 'technische systeem' vindt plaats i****n overleg met de verstrekker of operator****. Het doel is om de impact voor de verstrekker of operator tot een minimum te beperken en* ***het meest passieve systeem te gebruiken*** *(het gebruik van een test access point krijgt dan de voorkeur boven port mirroring).*
Het filteren gebeurt daarentegen in twee fasen: soft filtering bij de verstrekker met behulp van bijvoorbeeld packet brokers en hard filtering binnen de geclassificeerde infrastructuur van de ADIV op basis van andere tools, applicaties en apparatuur." (vetgedrukt door de Autoriteit)

55. Ten slotte werd de aanvrager, na de inschakeling van de door de Autoriteit aangewezen deskundige, in dit verband voor de derde en laatste keer ondervraagd[43]. Hij antwoordde met name het volgende:

---

[42] Wordt de configuratie van dit "technische systeem" ook bepaald door de ADIV en heeft de operator dus geen enkele controle hierover? Om welke technologie gaat het bij dit "technische systeem" (TAP, SPAN, NPB, andere)?

[43] Er werd gevraagd om per type dienst het volgende aan te geven:

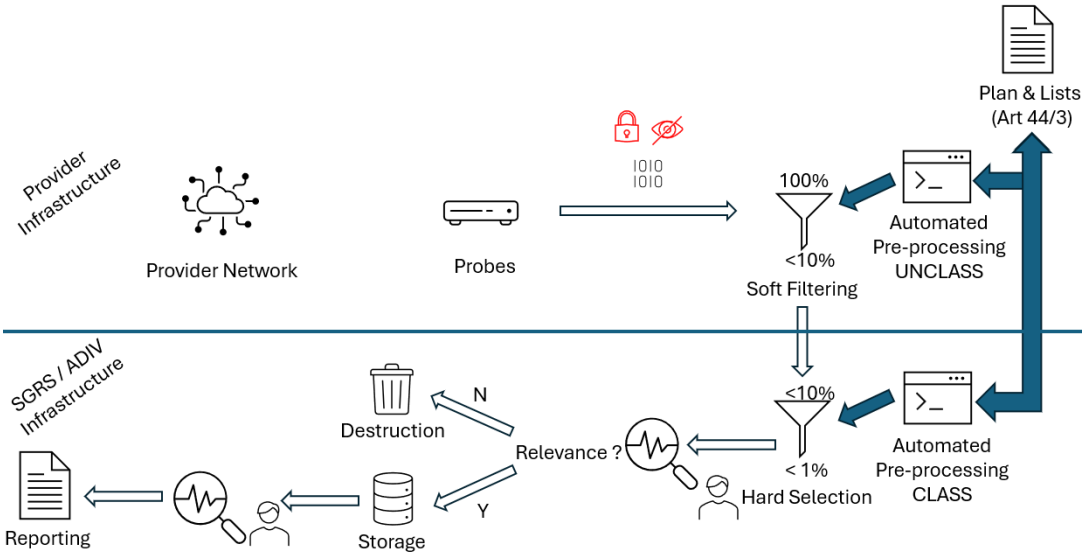
- het type technische maatregel/apparaat (of iets anders? – een verzoek?) dat men overweegt in te voeren, en de filtercapaciteit ervan met betrekking tot de interceptie van de betreffende communicatie;
- en het soort verzoek met betrekking tot het opheffen van de eventueel toegepaste versleuteling (met name, afhankelijk van het geval, of het gaat om een verzoek aan de dienstverstrekker om de ontsleutelde communicatie door te geven (in welk geval de dienstverstrekker de ontsleuteling uitvoert – a priori niet gezien het doel om geen informatie aan de dienstverstrekker door te geven) of om het ontsleutelingsmiddel (de sleutel(s)) door te geven),

en dit al naargelang de betrokken dienstverstrekker al dan niet over de relevante infrastructuur op Belgisch grondgebied beschikt.

Concreet rijzen deze vragen met betrekking tot de volgende soorten diensten:

"*Het koninklijk besluit heeft tot doel het algemene kader en de uitvoeringsbepalingen vast te stellen voor de beoogde samenwerking met de operatoren/verstrekkers en is dus niet bedoeld om de technische details van alle* ***mogelijke samenwerkingsvormen*** *te beschrijven, aangezien* ***elke operator/verstrekker op dit vlak anders is*** *(vandaar de noodzaak om een specifiek samenwerkingsakkoord te sluiten over de modaliteiten die niet onveranderlijk in het koninklijk besluit kunnen worden vastgelegd).* […]

De onderstaande figuur geeft een overzicht van de algemene werking van de beoogde samenwerkingsverbanden:



Met betrekking tot de verschillende diensten waarvan hieronder sprake is, is het van essentieel belang te begrijpen dat de ***focus ligt op alle digitale communicatie die mogelijk wordt gemaakt via het internetprotocol*** *(zie ook de definitie in het ontwerp van koninklijk besluit).*

- Communicatiedienst (gegevensverbindingslaag); internetdienst (IP); MPLS Multiprotocol Label Switching-dienst; telefoondiensten (3G-4G-4G); satellietcommunicatiediensten; VPN/proxy/Tor/mixnet-diensten;
- e-maildienst zonder end-to-end-versleuteling (zoals Gmail);
- e-maildienst met end-to-end-versleuteling (zoals Proton);
- instant messaging-dienst zoals Signal (minimale opslag van metagegevens);
- instant messaging-dienst zoals WhatsApp (grotere opslag van metagegevens);
- sociale netwerkdiensten.

Omvat de interceptie ook het onderscheppen van berichten met betrekking tot routing (BGP), domeinnamen (DNS) en certificeringsinstanties (CA)?

De samenwerking die zal worden opgezet en de medewerking van de operator/verstrekker staan echter volledig los van de bovenste lagen van het OSI-model en voor verstrekkers/operatoren zal er geen onderscheid worden gemaakt tussen al dan niet versleutelde communicatie, van het type applicatie (Signal, Whatsapp, enz.) of niet.

Dienstverstrekkers en netwerkoperatoren zullen verantwoordelijk zijn voor het installeren van TAP's (probes op het bovenstaande schema) binnen hun architectuur om het** door de ADIV gevraagde **relevante verkeer** **te dupliceren.

Dit verkeer wordt doorgestuurd naar de ADIV-apparatuur bij de operator of verstrekker, die de functie van filter vervult (overeenkomstig de artikelen 44 en 44/3).
***Het filteren is een verantwoordelijkheid van de ADIV** en wordt dus niet beschreven in dit ontwerp van koninklijk besluit, dat zich beperkt tot de modaliteiten betreffende de medewerking van de operatoren en dienstverstrekkers.*
Bovendien zijn de gebruikte technieken en instrumenten geheim en kunnen ze dus niet in deze e-mail of in een niet-geheim koninklijk besluit worden beschreven.

We geven u toch een korte uitleg over de beoogde filtering en verwerking in het kader van de samenwerkingen die via dit koninklijk besluit worden geregeld (het volgende zou eventueel in het ontwerp van koninklijk besluit kunnen worden opgenomen om de beoogde samenwerking te verduidelijken).
*De **eerste filtering, geautomatiseerd** en uitgevoerd met behulp van bijvoorbeeld packet brokers (pass/drop), al dan niet in combinatie met andere filterapparatuur, voert een eerste **niet-geclassificeerde** filtering uit om het verkeer te isoleren dat niet wettelijk is toegestaan en/of niet bruikbaar is voor de ADIV (**bijvoorbeeld** versleutelde communicatie waarbij alleen de eerste bytes van een versleutelde verbinding kunnen worden geregistreerd) Deze eerste filtering kan fijnmazig zijn (in het geval van indicatoren voor niet-geclassificeerde cyberdreigingen) of grover (IP-bereik / BGP-gebied / Domain Names, enz. van gebieden van belang).*
*Een **tweede (geautomatiseerde)** filtering met behulp van andere instrumenten en apparatuur (die niet hoeven te worden beschreven in het kader van dit koninklijk besluit, dat uitsluitend de verwachte medewerking van de operatoren en dienstverstrekkers beschrijft) zal plaatsvinden op de geclassificeerde architectuur van de ADIV om **uitsluitend** gericht te zijn op het verkeer van de organisaties en groeperingen die zijn opgenomen in de lijsten bedoeld in artikel 44/3.* ***Deze tweede filtering is geclassificeerd en uiterst nauwkeurig.***
***Na deze tweede filtering** volgt een verwerkingsperiode van zes maanden, zodat de medewerkers van de ADIV de relevantie van de gegevens die via de twee filteringsfasen zijn verzameld en voorbewerkt, kunnen beoordelen. Niet-relevante gegevens worden verwijderd*

(door herschrijving), terwijl relevante gegevens worden opgeslagen voor verdere analyse en rapportage.

[…].

Wat de andere vragen betreft:

1. […][44].
2. […][45].
3. *Ten slotte kunnen berichten met betrekking tot routing, domeinnamen en certificeringsinstanties worden onderworpen aan interceptie als er een effectief verband bestaat tussen bepaalde van deze berichten en de lijsten bedoeld in artikel 44/3.*" (vetgedrukt en onderstreept door de Autoriteit)

56. Het ontwerp en de aanvullende informatie die door de aanvrager is verstrekt, geven aanleiding tot de volgende opmerkingen van de Autoriteit.

II.4.3 Analyse en standpunt van de Autoriteit

57. **Ten eerste** begrijpt de Autoriteit uiteraard dat een normatief kader (wet of koninklijk besluit) niet alle technische details van de **voorgenomen gegevensverwerkingen** hoeft te omvatten, maar zij moet deze wel **concreet kunnen begrijpen om goed te kunnen beoordelen** of het normatieve kader geschikt is en of deze verwerkingen en dit kader voldoen aan de regels inzake gegevensbescherming die onder de bevoegdheid van de Autoriteit vallen. In het onderhavige geval is de Autoriteit er zich terdege van bewust dat zij niet bevoegd is om toezicht te houden op de gegevensverwerking door de inlichtingen- en veiligheidsdiensten, die onder de bevoegdheid van het Comité I vallen. Dit gezegd zijnde, is de Autoriteit wel bevoegd ten aanzien van de verwerking van gegevens door operatoren en verstrekkers van elektronische-communicatiediensten in het kader van hun eigen activiteiten wanneer deze verplicht zijn samen te werken met de bovengenoemde diensten, zoals zij eerder heeft aangegeven[46].

58. In dit verband is de Autoriteit van mening dat in dit advies ook moet worden gewezen op het **volgende standpunt dat het Comité I in punt 11 van zijn eigen advies heeft ingenomen**:

[44] Voor deze passage, zie punt 26.

[45] Zie het antwoord in punt 16.

[46] Zie punt 41.

"***<u>De burger</u>* 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 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.*" (vetgedrukt en onderstreept door de Autoriteit, cursief verwijderd om in overeenstemming te zijn met het cursief in de orginele tekst)

59. **De Autoriteit is het eens met het advies van het Comité I**: het ontwerp moet in die zin worden aangepast.

60. **Ten tweede wordt van operatoren en verstrekkers van elektronische-communicatiediensten verwacht dat zij** persoons**gegevens verwerken**. Overeenkomstig de AVG[47] (en niet alleen[48]) is een dergelijke "verwerking": "*een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens*". De betrokken operator of verstrekker moet echter (ervan uitgaande dat dit een doorslaggevend criterium is, quod non, is de rol van de operator in dit opzicht hoe dan ook zeer actief) op zijn netwerkinfrastructuur een (of meerdere) "*technisch(e) systeem(en)*" plaatsen (waarnaar de aanvrager ook verwijst met de termen "*technische oplossing*" of "*technisch mechanisme*") waarmee elektronische communicatiedatastromen 'naar' apparatuur van de ADIV die zich "*bij*" deze dienstverlener bevindt, kunnen worden gedupliceerd.

[47] Artikel 4.2) van de AVG.

[48] Zie in dit verband de andere regels inzake de bescherming van persoonsgegevens.

61. **Ten derde** begrijpt de Autoriteit dat het ingevoerde interceptiesysteem de **volgende drie selectie-/filterfasen** omvat, waarvan de laatste twee, in de huidige structuur van het ontwerp, niet onder haar bevoegdheid vallen:

    - In de eerste plaats **selecteert en dupliceert** het **technische systeem** dat door de operator of verstrekker van elektronische-communicatiediensten op zijn netwerkinfrastructuur is geïnstalleerd, **op geautomatiseerde wijze** "*bepaalde gegevensstromen*" (**met inbegrip van de inhoudsgegeven**s van de communicatie), "*in het buitenland verzonden of ontvangen elektronische communicatie*" of "*verkeer van belang*" voor de ADIV, bestemd voor apparatuur van de ADIV (voor een eerste filtering); hierna "**de selectie van gegevensstromen**";

    - Vervolgens wordt een **eerste geautomatiseerde en niet-geclassificeerde filtering** uitgevoerd door de ADIV, via apparatuur die **bij de betrokken operator of verstrekker** van elektronische-communicatiediensten is **geplaatst** ("*soft filtering*"); hierna "**de eerste filtering**";

    - Ten slotte vindt er een **tweede** – volgens de aanvrager "**uiterst nauwkeurige**" – **geautomatiseerde en geclassificeerde filtering** plaats op de geclassificeerde architectuur van de ADIV om uitsluitend gericht te zijn op het verkeer van de organisaties en groeperingen die in de relevante lijsten zijn opgenomen ("*hard selection*"); hierna "**de tweede filtering**".

62. **Ten vierde**, wat **de selectie van de gegevensstromen** betreft, zijn de criteria voor de configuratie van het (of de) "technische syste(e)m(en)" dat (die) door de operator (op een of meer nog te bepalen plaatsen van zijn netwerk) moet (moeten) worden geïnstalleerd om specifiek bepaalde soorten van deze communicatie te selecteren, namelijk het verkeer dat voor de ADIV van belang is, **onbepaald**. **Noch de I&V-wet, noch het ontwerp, noch de antwoorden van de aanvrager stellen de Autoriteit in staat om vast te stellen op basis van welke concrete/technische criteria en in welke omstandigheden** het door de operator geïnstalleerde "technische systeem" **de relevante gegevensstromen zal selecteren voor verdere filtering door de ADIV, afhankelijk van het type dienst in kwestie.** Met andere woorden, de Autoriteit is niet in staat om **het onderscheidende/filterende/gerichte vermogen – en de mate van dat vermogen – van de te installeren technische systemen** te identificeren met betrekking tot alle gegevensstromen die via de infrastructuur van de bij het ontwerp betrokken dienstverstrekkers worden doorgegeven.

63. Hoe dan ook, **juridisch gezien kan het ontwerp niet bepalen dat** "*de verstrekker van een elektronische-communicatiedienst of de netwerkoperator [...] een technisch systeem [...] [opzet] dat de automatische overdracht garandeert van stromen van gegevens en metagegevens van in het buitenland verzonden of ontvangen communicatie*". Ten eerste **weerspiegelt deze formulering niet de**

nuances die door de aanvrager zijn meegedeeld, hoe ontoereikend die ook mogen zijn. Ten tweede, en belangrijker nog, is een dergelijke bepaling **in strijd met het arrest van het Hof van Justitie van 6 oktober 2020, Privacy International**[49]. Zij laat namelijk de deur open voor een **algemene en ongedifferentieerde overdracht** van metagegevens van elektronische communicatie **en bovendien, in dit geval**, van **inhoudsgegevens**. De normatieve voorwaarde dat de betrokken communicatie **in het buitenland moet worden verzonden of ontvangen (met inbegrip** van het geval waarin de communicatie **in het buitenland wordt verzonden en ontvangen**), **ervan uitgaande dat deze daadwerkelijk kan worden toegepast (wat de aanvrager niet aantoont**, met name gelet op het type dienst in kwestie), is **buitensporig algemeen en kan leiden tot de onevenredige interceptie** van zeer grote hoeveelheden elektronische communicatie die geen enkel verband houden met de opdrachten van de ADIV. Zo kan bijvoorbeeld zonder onderscheid alle communicatie die vanuit land A wordt verzonden, die in land A wordt ontvangen en die in dat land A wordt verzonden en ontvangen, en die via de betrokken diensten worden doorgegeven, worden bedoeld. **De Autoriteit sluit zich op dit punt aan bij de negatieve conclusie van de CBPL in 2016, in punt 37 van haar advies**[50]. Zij wil wijzen op de volgende passage uit het **verslag van de door de Autoriteit aangewezen deskundige, die zij eveneens onderschrijft**:

> "*De gekozen strategie, waarbij potentieel zeer omvangrijke communicatiestromen bij de operatoren worden gedupliceerd en vervolgens in twee stappen gefilterd,* ***brengt een ernstig risico mee op informatievergaring op grote schaal of "mass surveillance".*** *Het voorbeeld dat gegeven worden in de toelichting is het afluisteren van de communicatie van de intelligentiedienst van Redland is inderdaad zeer redelijk, maar het is even goed mogelijk dat het gaat om de communicatie van een volledig land of zelfs een volledig continent.* ***Het feit dat de twee stappen van filtering onder volledige controle van ADIV gebeuren, betekent dat het niet kan uitgesloten worden dat gegevens op grote schaal verwerkt worden,*** *in een systeem vergelijkbaar met XKeyscore (NSA) of Tempora (GCHQ) zoals beschreven in de documenten gelekt door Snowden. Ook bestaat er het risico dat deze gegevens worden gedeeld met derde landen."* (vetgedrukt door de Autoriteit)

64. A priori **lijkt het er in ieder geval op dat de eerste** (niet-geclassificeerde) **filtering door de operator of de verstrekker van elektronische-communicatiediensten zelf moet worden uitgevoerd**, en niet door de ADIV. **En het toepasselijke normatieve kader, in principe de I&V-wet, zou hierin moeten voorzien.** In dit verband zou met name **de granulariteit/omvang** van de

[49] Zaak C-623/17.

[50] Zie punt 9.

potentieel betrokken "**geografische gebieden**" moeten worden vastgesteld. **De Autoriteit ziet echter af van een analyse van dit onderwerp** (bij gebrek aan voldoende informatie ter zake).

65. Het toepasselijke normatieve kader moet voorzien in de **mededeling aan operatoren en verstrekkers van elektronische-communicatiediensten van criteria die in overeenstemming zijn met de rechtspraak van het Hof van Justitie** inzake afwijkingen van de vertrouwelijkheid van elektronische communicatie, **op basis waarvan zij via hun systemen de elektronische communicatie selecteren die moet worden onderschept en doorgestuurd** naar de apparatuur van de ADIV, **binnen de grenzen van wat** voor deze laatste **noodzakelijk is** voor de uitoefening van zijn opdrachten. En zoals de Autoriteit al eerder benadrukte: "*En de noodzaak om gegevens te verwerken zal in concreto worden **beoordeeld in het licht van het doel van de verwerking** en de fase waarin de betreffende taak wordt uitgevoerd (de noodzaak van een gegeven kan variëren afhankelijk van de inlichtingencyclus; met name het feit dat een gegeven niet langer nodig is in een latere fase waarin de betreffende taak wordt uitgevoerd, betekent niet dat het in de beginfase niet nodig was*)." (in dit advies vetgedrukt door de Autoriteit)[51]

66. In deze context **betwijfelt de Autoriteit of het in het algemeen mogelijk is om in één enkele bepaling alle mogelijke scenario's te regelen, ongeacht het type dienst waar het om gaat** (Communicatiedienst (gegevensverbindingslaag); Internetdienst (IP); MPLS Multiprotocol Label Switching-dienst; telefoondiensten (3G-4G-4G); satellietcommunicatiediensten; VPN/proxy/Tor/mixnet-diensten; e-maildienst zonder end-to-end-versleuteling (zoals Gmail); e-maildienst met end-to-end-versleuteling (zoals Proton); instant messaging-dienst zoals Signal (minimale opslag van metagegevens); instant messaging-dienst zoals WhatsApp (grotere opslag van metagegevens); sociale netwerkdiensten). In ieder geval moet **voor elk type dienst goed worden nagedacht**. De Autoriteit meent te begrijpen dat het ontwerp hoofdzakelijk is opgesteld met het oog op de operatoren.

67. **Ten vijfde** begrijpt de Autoriteit, gezien de opdrachten van de ADIV, dat **het doel is om de uitwisseling van informatie** met operatoren en verstrekkers van elektronische-communicatiediensten **tot een minimum te beperken**. De Autoriteit heeft er echter al op gewezen[52] dat **het vragen van de medewerking** van verstrekkers van elektronische-communicatiediensten in het kader van de verwerking van persoonsgegevens **per definitie een uitwisseling van informatie met hen inhoudt**. Als verwerkingsverantwoordelijken zijn zij verplicht toe te zien op de rechtmatigheid van de gegevensverwerkingen die zij uitvoeren op grond van de wettelijke verplichting die op hen rust.

---

[51] Advies nr. 34/2024 van 15 april 2024 betreffende een wetsvoorstel tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en de wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten (CO-A-2024-139), punt 28.

[52] Zie (verleende) machtiging nr. 001/2025 van 18 juli 2025 *betreffende een machtigingsaanvraag zoals bedoeld in artikel 21, § 4, van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid: "Command-and-Control servers communicatiemetadata – waarschuwing"* (AH-2025-0034), punt 89.

68. Het **Belgische recht voorziet echter in specifieke waarborgen die rekening houden met het gevoelige karakter van de samenwerking** (met name) met de inlichtingen- en veiligheidsdiensten, namelijk: de artikelen 36 en 37 van de **I&V-wet** voorzien in een geheimhoudingsplicht; artikel 127/3 van de **wet van 13 juni 2005 betreffende elektronische communicati**e voorziet in de oprichting bij elke operator van een coördinatiecel die belast is met het verstrekken van elektronische-communicatiegegevens aan de wettelijk bevoegde autoriteiten, op hun verzoek (zie in het bijzonder paragraaf 2); de artikelen 11, 12 en 13 van de **WVG zelf** voorzien in een reeks afwijkingen van de rechten van de betrokkenen met betrekking tot gegevens die worden verwerkt door entiteiten die op enigerlei wijze samenwerken met de inlichtingen- en veiligheidsdiensten, terwijl artikel 92 van de WVG andere verplichtingen van deze entiteiten beperkt; en ten slotte regelt de **wet van 11 december 1998** ***betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst***, de bescherming van geclassificeerde informatie.

69. Concluderend is de Autoriteit van mening dat het ontwerp aanzienlijk moet worden aangepast. Meer fundamenteel zouden de artikelen 44 en 44/5 van de I&V-wet zelf op dit punt moeten worden verduidelijkt. **De medewerking van netwerkoperatoren en verstrekkers van elektronische-communicatiediensten in het kader van de artikelen 44 en 44/5 van de I&V-wet en het ontwerp moet het voorwerp uitmaken van een geactualiseerd parlementair debat** en worden geregeld door ondubbelzinnige normatieve bepalingen.

70. Deze vaststellingen doen uiteraard geen afbreuk aan de mogelijkheden tot gegevensverwerking die de ADIV zelf kan uitvoeren, in het buitenland of in België, onder zijn exclusieve verantwoordelijkheid (d.w.z. zonder de medewerking van de betrokken operatoren en verstrekkers), overeenkomstig de I&V-wet, verwerkingen die, ter herinnering, niet onder de bevoegdheid van de Autoriteit vallen, maar wel onder die van het Comité I.

OM DEZE REDENEN,
is de Autoriteit de volgende mening toegedaan:

1. Er moet in eerste instantie worden verwezen naar het advies van de CBPL van 2016 over het ontwerp dat later de wet van 2017 is geworden, en naar het afwijzende standpunt van de CBPL over artikel 44/5 van de I&V-wet (**punten 8-9**);

2. In overeenstemming met het standpunt van de Raad van State en gezien de inmenging die wordt veroorzaakt door de artikelen 44 en 44/5 van de I&V-wet, de uitvoering van deze bepalingen en de medewerking van operatoren en verstrekkers van elektronische-

communicatiediensten, moeten de opdrachten van de ADIV bedachtzaam en met strikte inachtneming van de beginselen van subsidiariteit en evenredigheid worden geïnterpreteerd (**punten 10-12**);

3. Het dispositief van het ontwerp moet worden aangepast en verduidelijken dat alleen de interceptie van elektronische communicatie die via de in België toegankelijke diensten van de betrokken operator of verstrekker verloopt, is toegestaan. Het moet aangeven dat het zich beperkt tot samenwerking met operatoren en verstrekkers van elektronische communicatiediensten die hun diensten in België aanbieden en daartoe gebruikmaken van een technische infrastructuur die relevant is voor de betrokken dienst of het betrokken netwerk, op het Belgische grondgebied en waarover zij voldoende controle uitoefenen, rekening houdend met de voorgenomen samenwerking. Wat betreft de soorten diensten in kwestie, is het de bedoeling dat de voorziene samenwerking in brede zin van toepassing is op iedereen die een dienst verleent waarbij zijn klanten de mogelijkheid wordt geboden om elektronisch informatie uit te wisselen (**punten 13-17**);

4. Het dispositief van het ontwerp bevat geen verplichting voor operatoren en verstrekkers van elektronische communicatie om mee te werken aan het ontcijferen van de elektronische communicatie die uiteindelijk wordt onderschept. Indien het de bedoeling van de auteur van het ontwerp is om in deze samenwerking te voorzien, moet hij het dispositief van het ontwerp aanpassen, rekening houdend met de ontwikkelingen in dit advies. In het ontwerp moet ten minste expliciet worden bepaald dat: ten eerste, de medewerking aan het ontcijferen van de betrokken elektronische communicatie alleen betrekking heeft op de technische versleutelingsoplossing die door de betrokken operator of verstrekker van elektronische-communicatiediensten zelf wordt gebruikt; ten tweede, deze medewerking niet mag leiden tot een vermindering van de kwaliteit van de door deze operator of verstrekker gekozen technische versleutelingsoplossing voor andere gebruikers wier elektronische communicatie niet moet worden onderschept; en ten derde de medewerking van de operator of verstrekker niet mag worden gevraagd voor het ontsleutelen van communicatie die end-to-end of op applicatieniveau is versleuteld. Dit onderwerp zou het voorwerp moeten uitmaken van een geactualiseerd parlementair debat (**punten 18-29**);

5. Het is aan de Raad van State om zich uit te spreken over de conformiteit van het ontwerp met het internationaal publiekrecht, en op basis van diens conclusies is het aan de auteur van het ontwerp om hieruit consequenties te trekken met betrekking tot de rechtmatigheid van de beoogde gegevensverwerkingen (**punten 30-31**);

6. Op basis van de verstrekte en beschikbare informatie kan de Autoriteit geen uitspraak doen over de vraag of de artikelen 44 en 44/5 van de I&V-wet moeten worden onderworpen aan een minder strenge ad-hocregeling voor voorafgaande controle dan de controle die van toepassing is op uitzonderlijke methoden voor het verzamelen van gegevens. Op dit punt is het raadzaam om het Comité I te raadplegen en daaruit consequenties te trekken met betrekking tot de rechtmatigheid van de beoogde verwerkingen. In ieder geval moet de motivering van het huidige wettelijk kader absoluut worden onderbouwd (**punten 32-39**);

7. Gezien de aanzienlijke inbreuk die de artikelen 44 en 44/5 van de I&V-wet maken op de rechten en vrijheden van de betrokkenen, ziet de Autoriteit niet op welke basis, in het licht van de Europese rechtspraak inzake afwijkingen van de vertrouwelijkheid van elektronische communicatie, het gerechtvaardigd zou zijn om de ADIV vrij te stellen van een voorafgaande beslissing (toestemming) van de BIM-commissie (of het Comité I), behalve in dringende gevallen, overeenkomstig de wijze waarop het gebruik van uitzonderlijke methoden voor het verzamelen van gegevens in het positieve recht is geregeld. Het Comité I moet de nodige tijd en financiële, technische en personele middelen krijgen om de door het ontwerp georganiseerde controle uit te voeren (**punten 41-47**);

8. Het ontwerp moet voldoen aan de vereiste van technische uitlegbaarheid overeenkomstig punt 11 van het advies van het Comité I en de autoriteit moet in staat zijn om de beoogde verwerkingsactiviteiten te begrijpen (**punten 58-59**);

9. In zijn huidige vorm is het ontwerp onevenredig, aangezien het de onevenredige selectie en omleiding van gegevensstromen die geen verband houden met de opdrachten van de ADIV naar de apparatuur van deze dienst mogelijk maakt. Het toepasselijke normatieve kader moet voorzien in de mededeling aan operatoren en verstrekkers van elektronische-communicatiediensten van criteria die in overeenstemming zijn met de rechtspraak van het Hof van Justitie inzake afwijkingen van de vertrouwelijkheid van elektronische communicatie, op basis waarvan deze dienstverstrekkers via hun systemen de elektronische communicatie die moet worden onderschept, selecteren en deze doorsturen naar de apparatuur van de ADIV, binnen de grenzen van wat voor deze laatste noodzakelijk is voor de uitoefening van zijn opdrachten. Het is noodzakelijk om hierover voor elk type dienst afzonderlijk goed na te denken (**punten 56-69**);

Deze vaststellingen doen uiteraard geen afbreuk aan de mogelijkheden tot gegevensverwerking die de ADIV zelf kan uitvoeren, in het buitenland of in België, onder zijn exclusieve verantwoordelijkheid (dat wil zeggen zonder de medewerking van de betrokken operatoren en verstrekkers), overeenkomstig de I&V-wet. Deze verwerkingen vallen, ter

herinnering, niet onder de bevoegdheid van de Autoriteit, maar wel onder die van het Comité I (**punt 70**);

10. In het licht van deze elementen en de ontwikkelingen in dit advies wordt aanbevolen dat de medewerking van netwerkoperatoren en verstrekkers van elektronische-communicatiediensten in het kader van de artikelen 44 en 44/5 van de I&V-wet en het ontwerp het voorwerp uitmaakt van een geactualiseerd parlementair debat en wordt geregeld door ondubbelzinnige normatieve bepalingen (**punten 29-69**).

Voor de Autorisatie- en Adviesdienst,
(get.) Alexandra Jaspar, Directeur