



ADVIES 2026/007 VAN 3 JUNI 2026

WETSONTWERP TOT WIJZIGING VAN DE INLICHTINGENWET EN DE CLASSIFICATIEWET

Gelet op het schrijven d.d. 29 april 2026 van de minister van Justitie aan het Comité R/I, overgemaakt via e-mail d.d. 30 april 2026, waarbij een adviesaanvraag wordt ingediend met betrekking tot het voorontwerp van wet 'tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en van artikel 16 van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst' (hierna: het wetsontwerp);

Bevoegdheid van het Comité R/I

Gelet op artikel 33, achtste lid van de Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;

Gelet op de artikelen 73, 95, 107 en 128 van de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

Te wijzigen rechtsnormen en adviesvoorstellen van het Comité

Het wetsontwerp beoogt diverse bepalingen van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (hierna: de Inlichtingenwet; afgekort: WIV) te wijzigen en toe te voegen. Daarnaast beoogt het wetsontwerp artikel 16 van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst (hierna: de Classificatiewet; afgekort: WCV) aan te vullen.

Naast een algemene beoordeling en een juridisch-technische en legistische beoordeling van de voorgestelde wettelijke bepalingen, die de volgorde van het wetsontwerp volgt, bevat voorliggend advies concrete adviesvoorstellen ([ADV-1 t.e.m. ADV-79](#)).

ADVIES

ALGEMENE BEOORDELING

1. Het Comité onderschrijft de noodzaak van een weerbare overheid die in staat moet zijn om het hoofd te bieden aan bedreigingen zoals spionage, inmenging, extremisme en terrorisme. Daarom staat het Comité in principe positief tegenover wetswijzigingen die nieuwe bevoegdheden verlenen aan de VSSE en de ADIV, zoals bijvoorbeeld de keuze om aan de inlichtingendiensten voortaan bepaalde actiebevoegdheden te verlenen, daar waar hun rol ter zake voorheen binnen de veiligheidsketen 'beperkt' bleef tot het inwinnen en analyseren van inlichtingen en deze ter beschikking stellen aan andere overheden om in voorkomend geval passend op te treden. Ook al is dit een ware paradigmashift, het Comité is van oordeel dat de vermenging van inlichtingen- en actiedienst een legitieme keuze kan zijn, maar dat enerzijds de operationele noodzaak duidelijker moet aangetoond worden in de memorie van toelichting, en anderzijds in het belang van de handhaving van de

democratische rechtsorde eveneens een versterking van de democratische controle op de inlichtingendiensten cruciaal is. Dit versterkt toezicht zal enerzijds een waarborg zijn voor de bescherming van de samenleving en van de rechten van individuele burgers, en zal anderzijds de inlichtingendiensten zelf behoeden voor onterechte verdachtmakingen. Deze bemerking geldt overigens ook voor andere nieuwe en verregaande bevoegdheden die in het ontwerp zijn opgenomen en die, samengenomen met de reeds bestaande mogelijkheden, deze diensten toelaten zeer gericht en krachtdadig op te treden. Maar de keerzijde van de medaille is natuurlijk dat er stevige garanties moeten zijn tegen mogelijk misbruik.

Het Comité herinnert er in dit verband aan dat in het federaal regeerakkoord ook de wens werd uitgedrukt om het democratisch toezicht op de inlichtingendiensten te verscherpen (federaal regeerakkoord 2025 -2029, blz. 142). Hoewel de Memorie van Toelichting meermaals verwijst naar het toezicht door de bevoegde organen ter verzekering van de fundamentele rechten, stelt het Comité vast dat dit voornemen onvoldoende werd gerealiseerd in het voorliggende voorontwerp. Het Comité dient integendeel vast te stellen dat tegenover de (legitieme) uitbreiding van de bevoegdheden van de inlichtingendiensten, onvoldoende aandacht werd besteed aan de kwaliteit van de nieuwe regelgeving en aan een passend, effectief en daadwerkelijk toezicht door het Comité of de BIM-Commissie, en dat zelfs bestaande waarborgen worden afgebouwd of afgeschaft. Het Comité kan hiermee niet akkoord gaan. Het noodzakelijk evenwicht tussen, enerzijds, uitgebreide bevoegdheden voor overheidsdiensten die opereren in een rechtsstaat, en anderzijds, het democratisch toezicht hierop zoals het een rechtsstaat betaamt, alsook de uitgesproken ambitie van de federale regering om het democratisch toezicht op de inlichtingendiensten te verscherpen, vereisen volgens het Comité dat de hierna volgende opmerkingen in het voorliggend ontwerp worden verwerkt.

(1) CYBER

2. De memorie van toelichting stelt: *“De technologieën die vandaag door kwaadwillige cyberactoren worden gebruikt, vereisen proactieve instrumenten die de Algemene Dienst Inlichting en Veiligheid (ADIV) en de Veiligheid van de Staat (VSSE) de bevoegdheid geven om doeltreffend te reageren op dreigingen uit cyberspace.”*¹ En verder: *“Gezien de steeds frequentere cyberaanvallen waaraan de Belgische openbare diensten in het algemeen en gevoelige diensten in het bijzonder worden blootgesteld, is het belangrijk om te beschikken over een juridisch kader dat deze diensten in staat stelt om hun opdrachten zo goed mogelijk uit te voeren.”*²

Het Comité erkent de noodzaak aan een afdoende sterk juridisch instrumentarium voor de inlichtingendiensten binnen het bestrijden van dreigingen in cyberspace. Onderstaande opmerkingen hebben louter betrekking op de juridische uitwerking hiervan.

Begrip technisch middel: technische verkenning en proactief onderzoek in cyberspace (ontwerp art. 3, 14° WIV)

3. Het Comité is van oordeel dat de invoeging voor de ADIV (en de VSSE)³ van een bevoegdheid om een “technische verkenning” en een technisch “proactief onderzoek” te verrichten, gerechtvaardigd is.

Het wetsontwerp voegt twee uitzonderingen toe aan de definitie van “technisch middel” in art. 3, 14° WIV:

¹ Memorie van toelichting, pag. 2.

² Memorie van toelichting, pag. 17.

³ Uit de memorie van toelichting lijkt deze wijziging vooral ten dienste te staan van de ADIV, in het bijzonder van het Cybercommando die hiervan deel uitmaakt.



“c) configuraties of apparaten die worden gebruikt om de technische staat, de kenmerken of de configuratie van informatica- en communicatiesystemen te zoeken en te analyseren op voor het publiek toegankelijke plaatsen in cyberspace” – te weten: het instrumentarium voor het proactief onderzoek in cyberspace

“d) configuraties of apparaten die worden gebruikt voor voorafgaande verkenning, functionele opsporing of analyse van kwetsbaarheden op voor het publiek toegankelijke plaatsen in cyberspace” – te weten: het instrumentarium voor de technische verkenning in cyberspace.

Het proactief onderzoek *“heeft tot doel om een technisch overzicht te krijgen van de blootstelling van systemen (gebruikte protocollen, open poorten, SSL/TLS-certificaten, enz.) Dit laatste is vergelijkbaar met een digitale topografische opmeting of een functionele inventaris van een netwerkzone. Dit onderzoek maakt het dus mogelijk om de technische vingerafdrukken van kwaadwillige actoren op te sporen, te identificeren en te valideren.”⁴⁵*

De technische verkenning *“bestaat meer bepaald uit het inventariseren van de technische kenmerken van een via internet toegankelijke informatica-infrastructuur, het identificeren van actieve technische diensten (zoals beheerinterfaces, mailservers of openbaar toegankelijke gegevensbanken), het registreren van de aangegeven of af te leiden softwareversies en het opsporen van elke configuratie die een in de vakliteratuur bekende kwetsbaarheid kan vertonen en van sporen van mogelijk misbruik door kwaadwillige actoren.”⁶*

Verder stelt de memorie van toelichting dat beide onderzoekshandelingen actueel onder de toepassing van art. 18/4, §1 WIV vallen (m.n. een observatie met behulp van technische middelen van voor het publiek toegankelijke plaatsen).⁷ Vervolgens bevat de memorie van toelichting een ruime beschrijving hoe betrokken handelingen in de praktijk werken en waarom de toelatingsprocedure van specifieke methoden hiervoor *de facto* onwerkzaam is. Deze toelichting overtuigt het Comité van de noodzaak van een wettelijke inrichting van beide handelingen alsook van het feit dat de procedure inzake specifieke methoden hiervoor niet is aangewezen.

Desondanks gaat het Comité niet akkoord met de wijze waarop dit wettelijk uitgewerkt wordt. Het Comité stelt immers vast dat er in het wetsontwerp geen daadwerkelijke wettelijke rechtsgrond voor betrokken onderzoeksbevoegdheden wordt gecreëerd. Juridisch-technisch worden er enkel twee aanvullende uitzonderingen gevoegd bij het begrip technisch middel. Dit begrip wordt in de Inlichtingenwet als criterium gehanteerd om de toepassing van bepaalde specifieke inlichtingenmethoden nader te bepalen (m.n. artt. 18/4, 18/5 en 18/7 WIV). Art. 3, 14° kan *an sich* nooit een rechtsgrond vormen voor een onderzoeksbevoegdheid.

De memorie van toelichting zelf maakt de vergelijking met het proactief en niet-intrusief scannen van openbaar toegankelijke netwerk- en informatiesystemen waardoor het Centrum voor Cybersecurity België (CCB) kwetsbare of onveilige geconfigureerde netwerk- en informatiesystemen kan opsporen, krachtens art. 19, 9° 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.⁸ Echter ook in deze wettelijke bepaling wordt betrokken onderzoekshandelingen omschreven als een bevoegdheid van het CCB, en niet als een uitzondering op een technisch middel.

Via deze weg wordt derhalve geen afdoende wettelijke rechtsgrond voor de twee vernoemde onderzoeksbevoegdheden ingericht, hoogstens wordt gezegd wat niet langer onder een huidige onderzoeksbevoegdheid valt (m.n. art. 18/4, §1 WIV). Door deze werkwijze in het wetsontwerp steunt een technische verkenning en een proactief onderzoek in cyberspace niet langer op een specifieke wettelijke grondslag doch louter op de permissieve regel (m.n. al wat niet expliciet verboden wordt, is toegelaten). In het licht van art. 8 EVRM

⁴ Eigen onderlijning van het Comité.

⁵ Memorie van toelichting, pag. 18.

⁶ Memorie van toelichting, pag. 19.

⁷ *Ibid.*

⁸ Memorie van toelichting, pag. 20.



en art. 22 Grondwet zijn betrokken onderzoeksverrichtingen evenwel te verregaand om louter te steunen op de permissieve regel. Om een afdoende rechtsgrond voor betrokken onderzoeksbevoegdheden te creëren moeten beide in een apart wetsartikel geregeld worden met een duidelijke opsomming van de toepasselijke voorwaarden en bijhorende controlemechanismen.

De werkwijze om uitzonderingen te voorzien in het begrip technisch middel zal er tevens voor zorgen dat betrokken handelingen volledig onttrokken worden van het toezicht van de BIM-Commissie, wat volgens het Comité niet gerechtvaardigd is.

Om alle boven vernoemde redenen is het Comité van oordeel dat de inzet van configuraties of apparaten binnen vernoemd proactief onderzoek of in het kader van vernoemde technische verkenning moet ingericht worden in een aparte wetsbepaling. Het Comité R/I adviseert om, naast het Comité (als tweedelijnscontroleur), de BIM-Commissie (als eerstelijnscontroleur) ter zake een corrigerende toezichtsbevoegdheid toe te kennen (ADV-1).

Computervredebreuk (ontwerp art. 44/6 WIV)

4. De memorie van toelichting stelt: “Artikel 44/1 machtigt de ADIV om in het kader van bepaalde opdrachten binnen te dringen in informaticasystemen in het buitenland. De huidige formulering geeft echter niet aan of deze intrusies kunnen plaatsvinden via tussenschakels zoals software, diensten of externe hostingproviders die verbonden zijn met de beoogde systemen. In de praktijk zijn de betreffende informaticasystemen echter bijna altijd afhankelijk van externe infrastructures die door derde partijen worden beheerd. Deze situatie leidt tot rechtsonzekerheid over de mogelijkheid om toegang te krijgen tot een systeem via een tool van een derde, terwijl het betrokken informaticasysteem wel degelijk een systeem is dat verband houdt met een organisatie of instelling als bedoeld in artikel 44/3.

De beoogde entiteiten beschikken namelijk niet noodzakelijkerwijs meer over interne servers of IT-infrastructuur. In de overgrote meerderheid van de gevallen worden hun systemen gehost op externe platforms, ondersteund door tools van derden (zoals e-maildiensten of IT-beveiligingsdiensten) of beheerd door technische onderaannemers. In deze context kan een echt doeltreffende intrusie vaak alleen worden uitgevoerd via deze technische tussenschakels, die dienen als indirecte toegang tot het uiteindelijke systeem. Bijvoorbeeld: als het doelwit een IT-dienstverlener inschakelt voor het beheer van zijn netwerk, vormt deze dienstverlener een potentieel toegangspunt tot het systeem.

Bij gebrek aan deze precisering kan de formulering van artikel 44/1 de bovengenoemde situatie niet expliciet dekken, zodat er in dit verband rechtsonzekerheid blijft bestaan. Het is belangrijk op te merken dat het gebruik van een derde partij geen schade toebrengt aan deze derde partij en dat dit in de meeste gevallen de enige manier is om toegang te krijgen tot het beoogde systeem. Er moet ook worden benadrukt dat de derde partij niet het doelwit is van de ADIV maar een middel vormt om toegang te krijgen tot het uiteindelijke systeem dat eigendom is van een instelling of organisatie die op de lijsten van artikel 44/3 staat. Ten slotte blijft deze mogelijkheid volledig gereguleerd, niet alleen door de in artikel 44/3 vermelde controles, maar ook door de opname van een specifieke controle op dit gebied in dezelfde bepaling. Dit zal het Comité I inzicht geven in de externe instrumenten die daadwerkelijk door de ADIV worden gebruikt, en dit in het kader van zijn achterafcontrole zoals bedoeld in bovengenoemd artikel.”⁹

Het ontwerp van art. 44/6, §1 WIV:

“De in artikel 44/1 bedoelde intrusie” – bedoeld wordt de intrusie in een informaticasysteem dat zich in het buitenland bevindt – “kan worden uitgevoerd met behulp van software, diensten of externe hosts die door het

⁹ Memorie van toelichting, pag. 81-82.



betrokken computersysteem worden gebruikt of daarmee verbonden zijn. Een dergelijke intrusie mag alleen worden uitgevoerd om technische redenen die noodzakelijk zijn om de optimale uitvoering van de opdracht te waarborgen of om de veiligheid van de opdracht of van de agent te garanderen.”.

5. Het Comité is van oordeel dat, wanneer toepassing wordt gemaakt van vernoemde regeling, er hierover een interne verslaggeving moet bestaan, dat dit bij wet moet worden voorgeschreven, en die te allen tijde beschikbaar wordt gehouden voor het Comité tijdens zijn bijzondere controle voorzien op deze speciale inlichtingenmethode (ADV-2).

6. Het Comité kon in de memorie van toelichting geen rechtvaardiging terugvinden waarom een dergelijke intrusie noodzakelijk zou zijn *“om de veiligheid (...) van de agent te garanderen”*.¹⁰ Het Comité adviseert om een dergelijke rechtvaardiging ofwel in de memorie toe te lichten ofwel om betrokken passage in de wetsbepaling te schrappen (ADV-3).

7. Aanvankelijk voorzag het interceptiesysteem, zoals gepland in de artikelen 44 en volgende van de WIV, in gerichte en niet-massale intercepties. Aangenomen wordt dat de controle door het Comité I volstaat om het gerichte en niet-algemene karakter te garanderen.¹¹

Echter, zoals de Gegevensbeschermingsautoriteit onlangs heeft opgemerkt in een van haar adviezen over een ontwerp van uitvoeringsbesluit van de WIV: *« 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. »*¹²

Onder deze omstandigheden verzoekt het Comité de wetgever om de interceptieregeling, zoals opgenomen in de artikelen 44 en volgende, te herzien. Hierbij moet met name rekening worden gehouden met de recente rechtspraak van het Hof van Justitie van de EU en het EHRM (meer bepaald het arrest in de zaak Centrum för Rättvisa t. Zweden, verzoekschrift nr. 35252/08) (ADV-4).

(2) DWINGENDE AFGIFTE VAN INFORMATIE DOOR PERSONEN EN ORGANISATIES DIE EEN DIENST VAN ALGEMEEN OPENBAAR BELANG VERRICHTEN

8. Het wetsontwerp beoogt de vorderingsbevoegdheid van de VSSE en de ADIV tegenover de openbare diensten (art. 14 WIV) te verduidelijken.¹³ De memorie van toelichting stelt: *“In het kader van de samenwerking met de inlichtingen- en veiligheidsdiensten wordt verduidelijkt welke instellingen een dienst van algemeen openbaar belang vervullen. Momenteel worden taken of diensten van openbaar belang niet langer uitsluitend door overheidsinstanties uitgevoerd. Het komt steeds vaker voor dat de uitvoering van deze taken van openbaar belang*

¹⁰ Eigen onderlijning van het Comité.

¹¹ « De minister van Landsverdediging merkt op dat het proportionaliteitsbeginsel nog steeds van toepassing is en dat het Comité I zeker zal optreden als de ADIV een beetje overal zou afluisteren. Het Comité I zou het Parlement op de hoogte brengen en eisen dat het niet-gerichte afluisteren onmiddellijk zou worden stopgezet. » (Parl. St., Senaat, 2002-2003, Verslag, 2-1412/3, p. 10).

¹² Advies GBA nr. 118/2025, nr. 63.

¹³ Memorie van toelichting, pag. 27.



wordt overgedragen aan particuliere of hybride organisaties. Om aan deze realiteit tegemoet te komen, worden verschillende bepalingen van de wet aangepast (artikelen 3, 29°, 14, 16 en 18/6/1).¹⁴

Concreet wordt in art. 3, 29° het begrip “de andere personen en organisaties die een dienst van algemeen openbaar belang verrichten” toegevoegd en omschreven. Wijzigingen worden gebracht aan de bevoegdheid tot het vorderen van informatie van openbare diensten (art. 14 WIV), tot het verzoeken van informatie van personen en organisaties die behoren tot de privésector (art. 16 WIV) en tot het vorderen van vervoers- en reisgegevens van private verstrekkers van vervoers- en reisdiensten (art. 18/6/1).

Art. 14, tweede lid WIV wordt als volgt gewijzigd (onderstreepte wordt toegevoegd):

“Op verzoek van een inlichtingen- en veiligheidsdienst, delen de gerechtelijke overheden, de ambtenaren en agenten van de openbare diensten, die van de politiediensten inbegrepen, en alle andere personen en organisaties die een dienst van algemeen openbaar belang verrichten voor het deel van hun activiteiten die voortvloeien uit deze dienst van algemeen openbaar belang, aan de betrokken inlichtingen- en veiligheidsdienst, de informatie mee die nuttig is voor de uitvoering van zijn opdrachten.”.

Het ontwerp van art. 3, 29° WIV definieert het begrip “de andere personen en organisaties die een dienst van algemeen openbaar belang verrichten” als:

“a) de personen die, ongeacht hun vorm en aard:

i) opgericht zijn met het specifieke doel te voorzien in behoeften van algemeen belang die niet van industriële of commerciële aard zijn, en;

ii) rechtspersoonlijkheid hebben, en;

iii) op een van de volgende wijzen afhangen van de Staat, de Gewesten, de Gemeenschappen, de lokale overheidsinstanties of andere overheids- of publiekrechtelijke instellingen:

1. ofwel worden hun werkzaamheden die de essentiële behoeften van de bevolking waarborgen in hoofdzaak gefinancierd door de Staat, de Gewesten, de Gemeenschappen, de lokale overheidsinstanties of andere overheids- of publiekrechtelijke instellingen;

2. ofwel is hun beheer onderworpen aan het toezicht van de Staat, de Gewesten, de Gemeenschappen, de lokale overheidsinstanties of andere overheids- of publiekrechtelijke instellingen;

3. ofwel zijn meer dan de helft van het bestuurs-, leidinggevende of toezichthoudende orgaan aangewezen door de Staat, de Gewesten, de Gemeenschappen, de lokale overheidsinstanties of andere overheids- of publiekrechtelijke instellingen;

b) de verenigingen bestaande uit de Staat, de Gewesten, de Gemeenschappen, de lokale overheidsinstanties of andere overheids- of publiekrechtelijke instellingen of uit een of meer personen bedoeld in het punt a);”.

In art. 16 WIV worden de woorden “en voor zover ze niet onder het toepassingsgebied van artikel 14 vallen” toegevoegd. Deze aanpassing zorgt ervoor dat de afgifte van informatie door alle private bedrijven en organisaties die diensten van algemeen belang verrichten in belangrijke mate verplicht wordt. Hierdoor vallen dergelijke actoren immers, voor wat betreft de gegevens verwerkt binnen de publieke taakstelling, niet langer onder de toepassing van art. 16 WIV (facultatieve afgifte) maar onder deze van art. 14 WIV (verplichte afgifte). Ter illustraties van het soort entiteiten die onder het begrip “personen en organisaties die een dienst van algemeen openbaar belang verrichten” vallen, verwijst de memorie van toelichting naar de bijlagen van de Cyberbeveiligingswet van 26 april 2024 waar diverse firma's in kritieke sectoren worden opgesomd.¹⁵ Op basis van de voorgestelde wettelijke definitie is het toepassingsgebied echter veel ruimer. Private firma's die door de voorziene wijzigingen verplicht worden informatie aan de VSSE en de ADIV te geven zijn bijvoorbeeld: de universiteiten en scholen (onderwijs)¹⁶, de havenbedrijven, notariskantoren, gerechtsdeurwaarderskantoren,

¹⁴ Memorie van toelichting, pag. 11.

¹⁵ Memorie van toelichting, pag. 27.

¹⁶ Ook vernoemd: memorie van toelichting, pag. 44.



woningcorporaties (sociale huisvesting), energiebedrijven (netbeheer), openbaar vervoersbedrijven, bepaalde zorginstellingen, mutualiteiten (bv. in het kader van het beheer van de werkloosheidsuitkeringen). Deze verplichte afgifte geschiedt in combinatie met een ontbreken van een voorafgaand, onafhankelijk en corrigerend toezicht (bv. door de BIM-Commissie).

In art. 18/6/1 WIV worden de woorden “*met uitzondering van deze die onder de toepassing van artikel 14 vallen*” toegevoegd. Het Comité stelt vast dat dit ervoor zorgt dat het inwinnen door de VSSE en de ADIV van een veelheid van informatie hierdoor niet langer onder het onafhankelijk en corrigerend BIM-toezicht staat van de BIM-Commissie en het Comité R/I (m.n. het verzamelen van vervoers- en reisgegevens bij de luchthavens). Door de toevoeging van vernoemde woorden in art. 18/6/1 verwordt deze specifieke methode *de facto* een gewone methode (art. 14 WIV). Het Comité herinnert eraan dat ingeval dezelfde informatie via de Passagiersinformatie-eenheid wordt opgevraagd, een voorafgaand akkoord van de BIM-Commissie wordt vereist (art. 16/3 WIV), zoals door de wetgever bepaald in navolging van het PNR-arrest van het Grondwettelijk Hof.¹⁷

In de memorie van toelichting wordt gesteld dat “*de reeds bestaande methoden voor het verzamelen van gegevens in de organieke wet op verschillende wijzen wordt gewijzigd.*”. Hierbij wordt toegevoegd dat “*de bescherming van fundamentele rechten gewaarborgd blijven*”.¹⁸ Minstens in het licht van de aanpassingen in art. 18/6/1 WIV kan het Comité niet akkoord gaan met deze stelling.

Het begrip “de andere personen en organisaties die een dienst van algemeen openbaar belang verrichten” (ontwerp art. 3, 29° juncto art. 14 WIV)

9. Het belang van de vorderingsbevoegdheid van de inlichtingendiensten (art. 14 WIV) wordt reeds lang aanvaard. Zo stelt de memorie van toelichting bij de BIM-wet van 4 februari 2010 reeds dat “*[r]ekening houdend met de opdracht van de inlichtingen- en veiligheidsdiensten die onder andere bestaat in het beschermen van de fundamentele belangen van de Staat, is het onontbeerlijk dat alle openbare diensten hun medewerking verlenen aan de inlichtingendiensten wanneer zij daar om vragen.*”.¹⁹ Over de draagwijdte van het begrip “openbare diensten” stelt de memorie van toelichting bij de Inlichtingenwet van 30 november 1998: “*Het begrip openbare dienst moet in de breedst mogelijke betekenis verstaan worden en behelst onder andere elke instelling van openbaar nut (...).*”²⁰ Een belangrijke kanttekening bij deze laatste verwijzing is dat de afgifte van informatie door openbare diensten in 1998 nog facultatief plaatsvond, en pas in 2010 verplicht werd.

10. Noch in 1998 noch in 2010 werd een debat gevoerd rond de exacte draagwijdte van het begrip “openbare diensten”. Nochtans bestaat er hieraan behoefte voor wat betreft de openbare diensten in functionele zin. Het Comité stelt vast dat het wetsontwerp het personele toepassingsgebied van de vorderingsbevoegdheid tegenover de openbare diensten (art. 14 WIV) wenst te verduidelijken door de toevoeging en omschrijving van het begrip “de andere personen en organisaties die een dienst van algemeen openbaar belang verrichten”. De memorie van toelichting stelt ter zake: “*De opstellers hebben zich voor de definitie geïnspireerd op het toepassingsgebied van de wet van 13 augustus 2011 inzake overheidsopdrachten en bepaalde opdrachten voor werken, leveringen en diensten op defensie- en veiligheidsgebied en op het toepassingsgebied 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.*”²¹ Het Comité brengt vooreerst onder de aandacht dat ook diverse andere

¹⁷ Grondwettelijk Hof, arrest nr. 131/2023 van 12 oktober 2023.

¹⁸ Memorie van toelichting, pag. 10.

¹⁹ Parl. St. Senaat 2008-2009, nr. 4-1053/1, 39.

²⁰ Parl. St. Kamer 1995-1996, nr. 49-638/001, 14.

²¹ Memorie van toelichting, pag. 27.

wetgevende teksten min of meer eenzelfde bepaling hebben, waaronder, doch niet uitsluitend, de Gegevensbeschermingswet van 30 juli 2018 (art. 5), de Overheidsopdrachtenwet van 17 juni 2016 (art. 2, 1°) en de Wet van 4 mei 2016 inzake open data en het hergebruik van overheidsinformatie (art. 2, 1°).

Het wetsontwerp maakt de legistische keuze om het begrip “openbare dienst” in art. 14 WIV te laten staan en het begrip “de andere personen en organisaties die een dienst van algemeen openbaar belang verrichten” hieraan toe te voegen.²² Hieruit volgt dat al de instanties die reeds onder eerstgenoemde begrip vallen – bv. de federale staat, de gemeenschappen, de gewesten, de provinciale en lokale overheden, en de openbare centra voor maatschappelijk welzijn – niet dienen ondergebracht te worden onder laatstgenoemde begrip. Echter, omwille van het feit dat de wetgever in vernoemde memories van toelichting eerder stelde dat het begrip “alle openbare diensten” omvat en “in de breedst mogelijke betekenis verstaan (moet) worden” (*supra*) in combinatie met het feit dat de praktijk nood voelt om dit begrip in de wet nader te verduidelijken, is het Comité van oordeel dat er beter geopteerd wordt om één begrip te kiezen en vervolgens dit begrip exhaustief te omschrijven (m.n. met alle categorieën die er onder vallen, organiek én functioneel) (ADV-5). Gezien het begrip “openbare diensten” momenteel reeds in art. 14 WIV wordt gebruikt en gelet op bestaande passages in vernoemde memories van toelichting is het verdere gebruik van dit begrip het meest aangewezen, aangevuld met een exhaustieve omschrijving ervan in art. 3, 29°.

Als dusdanig dienen dan ook de overheidsinstanties die deel uitmaken van de federale staat, de gemeenschappen, de gewesten, de provinciale en lokale overheden, en de openbare centra voor maatschappelijk welzijn expliciet vernoemd te worden.

De vraag stelt zich of volgende entiteiten er (nog) onder vallen: de hulpverleningszones, de prezones, de Brusselse agglomeratie, de meergemeentezones, de binnengemeentelijke territoriale organen, de Franse Gemeenschapscommissie, de Vlaamse Gemeenschapscommissie en de Gemeenschappelijke Gemeenschapscommissie.

Tot slot merkt het Comité op dat art. 5 Gegevensbeschermingswet ook nog spreekt over “*de rechtspersonen van publiek recht die van de Federale Staat, de deelstaten of lokale overheden afhangen*”, en dit los van de categorieën die reeds zijn ondergebracht onder het ontwerp van art. 3, 29°. Het Comité adviseert om een duidelijk antwoord te formuleren of ook deze onder de personele toepassing van art. 14 WIV dienen te vallen (ADV-6).

Het begrip “openbare sector”

11. Het huidige art. 14, laatste lid WIV stelt actueel:

“Met inachtneming van de geldende wetgeving kunnen de inlichtingen- en veiligheidsdiensten, overeenkomstig de door de Koning vastgelegde algemene nadere regels, toegang krijgen tot de gegevensbanken van de openbare sector die nuttig zijn voor de uitoefening van hun opdrachten.”

Het begrip “openbare sector” komt alleen op deze plaats in de Inlichtingenwet voor. In het licht van de wijzigingen voorzien in de rest van art. 14 WIV (*supra*) adviseert het Comité om dit begrip te verduidelijken) (ADV-7). De vraag rijst onder meer of het personele toepassingsgebied tussen de vorderingsbevoegdheid (ex. art. 14, tweede lid) en de toegangsregeling tot de gegevensbanken van de openbare sector (ex. art. 14, laatste lid) hetzelfde is, vooral dan wat betreft de gegevensbanken van de openbare diensten in functionele zin.

²² Eigen onderlijning van het Comité.



Private verstrekkers van vervoers- en reisdiensten (art. 18/6/1 WIV)

12. Volgens de memorie van toelichting wordt art. 18/6/1 WIV gewijzigd “om dit artikel in overeenstemming te brengen met het gewijzigde artikel 14 WIV”. Van belang in dit kader is dat de toelichting verduidelijkt dat “(d)e personen en organisaties die een dienst van algemeen openbaar belang verrichten in de vervoers- en reissector (zoals de luchthavens) (...) door de wijziging niet meer onder het toepassingsgebied van artikel 18/6/1 WIV (zullen) vallen maar onder artikel 14 WIV.”²³ Dit heeft ten gevolge dat een specifieke methode wordt omgevormd tot een gewone methode. Concreet stelt de memorie van toelichting “(zullen) (g)egevens met betrekking tot de “termac”-zone van de luchthaven (...) kunnen opgevraagd (worden) op grond van artikel 14 in plaats van op grond van artikel 18/6/1.”.

De keuzes van de BIM-wetgever in 2010 om in de Inlichtingenwet een logische structuur in te stellen voor wat betreft de onderzoeksbevoegdheden van de inlichtingendiensten – m.n. een onderscheid tussen uitzonderlijke, specifieke en gewone methoden naargelang de graad van privacy-inmenging – wordt door de voorgestelde wetswijziging opnieuw verlaten. Het Comité betreurt dit. Het zorgt er niet enkel voor dat de werking van de inlichtingenmethoden onoverzichtelijk wordt, het heeft eveneens ten gevolge dat er steeds minder externe, voorafgaande controle plaatsvindt op de inzet van intrusieve methoden bij de gegevensverzameling.

13. In de memorie van toelichting wordt verder gesteld: “Deze wijziging heeft geen invloed op de toepassing van de procedures, machtigingen en controles die momenteel in de organieke wet voor bijzondere gevallen zijn vastgelegd.”. Het Comité brengt onder de aandacht dat dit verkeerdelijk is. Omdat een specifieke methode wordt omgevormd tot een gewone methode wordt er niet langer een controle door de BIM-Commissie georganiseerd. Hierdoor worden er diverse controlemechanismen van toepassing bij specifieke methoden achterwege gelaten. Zo kan de Commissie een onwettig bevonden methode niet langer stopzetten en de exploitatie van onwettig ingewonnen gegevens niet langer schorsen. Als specifieke methode kan de betrokken methode ook niet worden uitgevoerd vooraleer de door het diensthoofd gedane beslissing aan de Commissie ter kennis werd gebracht. Deze kennisgeving zorgt ervoor dat de Commissie op de hoogte is gesteld van een geplande methode en onmiddellijk tussenbeide kan komen ingeval ze deze geplande of lopende methode onwettig bevindt. Een kennisgeving aan de BIM-Commissie (of aan het Comité) na het uitvoeren van deze methode kan een dergelijke voorafgaande kennisgeving aan de BIM-Commissie niet compenseren.

In het licht hiervan adviseert het Comité om ofwel de voorgestelde wijziging te schrappen, ofwel om de BIM-Commissie een vergelijkbare bevoegdheid toe te kennen met betrekking tot de vervoers- en reisgegevens die gevorderd worden op grond van art. 14 of 16 WIV (ADV-8).

Bij een uitbreiding van het personele toepassingsgebied van art. 14 en/of 16 WIV is het Comité van mening dat, voor wat betreft dit aspect, eveneens het advies van de Gegevensbeschermingsautoriteit dient ingewonnen te worden. De doorgifte van informatie vanuit de openbare respectievelijke private sector naar een inlichtingendienst betreft immers een verwerking van persoonsgegevens zoals bedoeld in titel 1 van de Gegevensbeschermingswet.

(3) ARTIFICIËLE INTELLIGENTIE: ONTWIKKELING EN GEBRUIK (ontwerp art. 12/1 – 12/5)

Algemeen

14. Het Comité stelt vast dat de uitwerking in het wetsontwerp met betrekking tot de ontwikkeling en het gebruik van artificiële intelligentie door de VSSE en de ADIV tijdens hun taakuitoefening zeer summier is; te

²³ Memorie van toelichting, pag. 59.



summier alvast om te corresponderen met de gerechtvaardigde doelstellingen geformuleerd in de memorie van toelichting. De regeling in de betrokken vijf wetsartikelen omvatten in wezen weinig concrete toepassingsvoorwaarden en controlemechanismen.

De memorie van toelichting stelt dat het wetsontwerp “een tweeledig doel (heeft): Enerzijds wil het de invoering bevorderen van mensgerichte en betrouwbare kunstmatige intelligentie, en tegelijkertijd de veiligheid en de grondrechten van de burgers te beschermen tegen de mogelijke risico's van AI. Anderzijds wil het de operationele behoeften ondersteunen van de inlichtingen- en veiligheidsdiensten, die een leidende rol willen spelen in de ontwikkeling en het gebruik van veilige, betrouwbare en ethische AI bij de uitvoering van hun taken.”²⁴ Het Comité juicht iedere gestelde doelstelling toe.

15. Het wetsontwerp voegt een definitie in van de begrippen “AI-systeem” (ontwerp art. 3, 14/1° WIV) en “AI-testomgeving” (ontwerp art. 3, 14°/2 WIV), die duidelijk gebaseerd zijn op de omschrijving van betrokken begrippen in de AI-verordening van de Europese unie²⁵ (art. 3, 1) resp. art. 3, 55) AI-verordening)).

De memorie van toelichting stelt: “Hoewel de Verordening (EU) 2024/1689 betreffende artificiële intelligentie (hierna “de AI-Verordening”) niet van toepassing is op het gebruik van AI-systemen door de inlichtingen- en veiligheidsdiensten voor de uitoefening van hun opdrachten, is de definitie in dit voorontwerp afgestemd op de definitie in de AI-Verordening en op de werkzaamheden van internationale organisaties die actief zijn op het gebied van AI, teneinde rechtszekerheid te waarborgen en convergentie te vergemakkelijken, terwijl tegelijkertijd de nodige flexibiliteit wordt geboden om rekening te houden met de snelle technologische ontwikkelingen op dit gebied.”²⁶

Het Comité merkt op dat in de AI-verordening de woorden “onder begeleiding van een toezichthouder” eveneens zijn aangebracht onder de definitie van “AI-testomgeving”. In licht van de memorie van toelichting²⁷ en het ontwerp art. 12/3, tweede lid WIV is het duidelijk dat de opsteller de ontwikkeling van AI door de inlichtingendiensten wenst te plaatsen onder het toezicht van het Comité R/I. Om die reden, en omwille van tekstuele duidelijkheid, adviseert het Comité om de woorden “onder toezicht van het Vast Comité I” toe te voegen aan de wettelijke definitie van het begrip “AI-testomgeving” (ADV-9). Het Comité gebruikt hierbij doelbewust het begrip “toezicht” en niet “begeleiding” omdat het van oordeel is dat onafhankelijk toezicht onverenigbaar is met het begeleiden van vernoemde proces.

16. Vanuit legistiek en inhoudelijk oogpunt is het voor het Comité niet duidelijk waarom de bepaling “De inlichtingen- en veiligheidsdiensten kunnen AI-systemen ontwikkelen en gebruiken voor de uitoefening van de opdrachten bedoeld in de artikelen 7, 8 en 11.” (ontwerp art. 12/1) en de bepaling “De ontwikkeling of het gebruik van AI-systemen is allen toegestaan als de waarborgen en voorwaarden in de artikelen 12/3 tot 12/5 zijn voldaan.” in twee aparte wetsartikelen staan. Omwille van de grotere zichtbaarheid dat beide bepalingen onlosmakelijk verbonden zijn adviseert het Comité om beide bepalingen in één wetsartikel te huisvesten (ADV-10).

Voorts wijst het Comité erop dat art. 8 WIV geen opdrachten van de VSSE bevat, doch louter de wettelijke definities van begrippen die gehanteerd worden in art. 7 WIV die wel de opdrachten van de VSSE bevat. Om

²⁴ Memorie van toelichting, pag. 15 (en 36).

²⁵ Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van (...) (verordening artificiële intelligentie), PbEU L van 12.7.2024.

²⁶ Memorie van toelichting, pag. 26.

²⁷ Memorie van toelichting, pag. 26 en 37.



die reden adviseert het Comité om de woorden “de artikelen 7, 8 en 11” in ontwerp art. 12/1 te vervangen door “de artikelen 7 en 11” (ADV-11).

Ontwikkeling van AI en het externe toezicht erop

17. Ontwerp art. 12/3 WIV stelt: “Elk AI-systeem dat door de inlichtingen- en veiligheidsdiensten wordt geïmplementeerd, moet zijn getest in een AI-testomgeving of aan een alternatieve maatregel zijn onderworpen voordat het in reële gebruiksomstandigheden wordt ingezet.

Het diensthoofd verstrekt het Vast Comité I de documentatie van de in het eerste lid bedoelde test of alternatieve maatregel.

De persoonsgegevens die oorspronkelijk voor een ander doel zijn verzameld, kunnen worden verwerkt voor de ontwikkeling, training en het testen van AI-systemen in de AI-testomgeving.”

Met betrekking tot de vernoemde controle van het Comité stelt de memorie van toelichting: “Deze documentatie wordt door het diensthoofd aan het Vast Comité I verstrekt in het kader van zijn controle zoals geregeld door de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse.”.²⁸ Het Comité is van oordeel dat in de memorie van toelichting én in het wetsontwerp expliciet moet toegevoegd worden dat de bedoelde controle geschiedt met inbegrip van de corrigerende bevoegdheden van het Comité zoals bedoeld in art. 51/3 van de Wet van 18 juli 1991 (ADV-12). Het betreffen de corrigerende bevoegdheden in het kader van zijn toezicht op de verwerking van persoonsgegevens en omvatten onder meer de bevoegdheid om een verwerkingsbeperking of -verbod ten opzichte van de inlichtingendiensten op te leggen. Zeker in het licht van het derde lid van ontwerp art. 12/3, dat voorziet dat de inlichtingendiensten persoonsgegevens kunnen aanwenden die voor een ander doel zijn verzameld, is een dergelijke toevoeging essentieel.

18. Ontwerp art. 12/4 omvat het voorschrift om een effectbeoordeling op de grondrechten uit te voeren voor elke inzet van AI-systemen. Het bevat tevens de verplichte aspecten van deze effectbeoordeling.

Opmerkelijk is dat de kern van een dergelijke effectbeoordeling, zijnde “een beschrijving van de specifieke risico’s op schade die waarschijnlijk gevolgen zullen hebben voor de categorieën natuurlijke personen of groepen van natuurlijke personen die mogelijk worden beoogd” ontbreekt. Ook wordt vereist dat “een beschrijving van de periode waarin en de periode waarvoor het AI-systeem zal worden gebruikt”, maar ontbreekt “een beschrijving van de frequentie waarmee het AI-systeem zal worden gebruikt”. Het Comité is van oordeel dat beide aspecten dienen te worden toegevoegd (ADV-13).

19. Gelet op de technische complexiteit van AI-systemen is het Comité van oordeel dat het, om toezicht te kunnen uitoefenen op een AI-systeem, noodzakelijk is dat het te allen tijde toegang krijgt en heeft tot de door mensen ingevoerde gegevens, de door het systeem gegenereerde resultaten en de onderliggende mechanismen van de gebruikte AI- en algoritmetstechnologieën, en in het bijzonder en op niet-limitatieve wijze:

- de trainingsgegevens en datasets;
- de logica van het model, de architectuur en de broncode ervan;
- de prestatie-indicatoren;
- de logbestanden (logs) en de audit- en wijzigingslogs van het systeem;

Wanneer er commerciële oplossingen worden gebruikt waarover de inlichtingendiensten geen volledige controle hebben, moet het Comité ten minste toegang hebben tot dezelfde informatie als de diensten en beschikken over een sandbox-omgeving waarin de besluitvormingstrajecten van het systeem kunnen worden geaudit (ADV-14)

²⁸ Memorie van toelichting, pag. 37.



20. Het Comité stelt vast dat het principe van menselijk toezicht in het ontwerp art. 12/5, eerste lid wordt ingebracht. Deze bepaling stelt: “*Elk gebruik van een AI-systeem wordt onderworpen aan een menselijke controle om elk risico op schending aan de grondrechten te beperken of voorkomen.*”.

Deze bepaling beperkt menselijk toezicht binnen het gebruik van AI, een vergelijkbare verplichting binnen de ontwikkeling van AI ontbreekt evenwel. Nochtans is dit fundamenteel. Vertrekkende vanuit art. 14 AI-verordening als inspiratiebron, adviseert het Comité om volgende principes in de wet in te schrijven (ADV-15):

- elk AI-systeem dat door de inlichtingen- en veiligheidsdiensten wordt geïmplementeerd, wordt zodanig ontworpen en ontwikkeld, met inbegrip van passende mens-machine-interface-instrumenten, dat hierop tijdens de periode dat zij worden gebruikt, op doeltreffende wijze toezicht kan worden uitgeoefend door natuurlijke personen;
- het menselijk toezicht is gericht op het voorkomen of beperken van de risico's voor de veiligheid of grondrechten die zich kunnen voordoen wanneer een AI-systeem wordt gebruikt in overeenstemming met het beoogde doel ervan of in een situatie van redelijkerwijs te voorzien misbruik;
- de toezichtmaatregelen worden gewaarborgd door middel van maatregelen die, waar technisch haalbaar, in het AI-systeem, worden ingebouwd voordat dit systeem in gebruik wordt gesteld;
- met het oog op de uitvoering van bovenstaande aspecten moet het AI-systeem zodanig worden ontwikkeld dat natuurlijke personen die verantwoordelijk zijn voor het menselijk toezicht, in staat worden gesteld om waar passend en evenredig:
 - a) de relevante capaciteiten en beperkingen van het AI-systeem goed te begrijpen en de werking ervan naar behoren te kunnen monitoren, onder meer met het oog op het opsporen en aanpakken van onregelmatigheden, storingen en onverwachte prestaties;
 - b) zich bewust te blijven van de mogelijke neiging om automatisch of te veel te vertrouwen op de output van een AI-systeem;
 - c) de output van het AI-systeem met een hoog risico juist te interpreteren, bijvoorbeeld de beschikbare instrumenten en methoden voor interpretatie;
 - d) in alle specifieke situaties te kunnen besluiten om het AI-systeem niet te gebruiken of de output van het AI-systeem met een hoog risico op andere wijze te negeren, door een andere beslissing te vervangen of terug te draaien;
 - e) in te grijpen in de werking van het AI-systeem of het systeem te onderbreken door middel van een stopknop of een vergelijkbare procedure waarmee het systeem op veilige wijze kan worden stopgezet.

Gebruik van AI en het externe toezicht erop

21. Het Comité stelt vast dat het wetsontwerp geen specifieke bepalingen bevat naargelang de verschillende soorten gebruik van AI binnen de uitvoering van de opdrachten. Zo is AI-gebruik niet enkel mogelijk binnen de informatiegaring, doch ook binnen de inlichtingenanalyse (bv. beoordelen van natuurlijke personen). Het wetsontwerp laat, onrechtstreeks, eveneens AI-gebruik toe binnen verstoringsacties (*infra*). Het Comité is van oordeel dat er in de Inlichtingenwet bijzondere controlemechanismen dienen te worden ingeschreven voor wat betreft dit AI-gebruik, waarbij de BIM-Commissie en het Comité R/I corrigerende bevoegdheden hebben bij een onrechtmatig gebruik ervan (bv. op basis van AI wordt een persoon als gevaarlijk gekwalificeerd hoewel er hiervoor geen objectieve informatie voorhanden is) (ADV-16).

22. De definitie van het AI-systeem sluit het gebruik van agentic AI (agent-gebaseerde AI) niet uit, die gekenmerkt wordt door een grotere autonomie en een groter vermogen tot interactie met de reële omgeving. Dit type AI kan op massale wijze gegevens en acties genereren, zelfs onder menselijk toezicht. Het risico is reëel dat het externe en onafhankelijke toezicht van het Comité, hetzij in realtime hetzij a posteriori, niet effectief



kan worden uitgeoefend. Een mogelijke oplossing is de implementatie, binnen het AI-systeem zelf, van monitoring-, rapporterings- en controlemechanismen die eveneens op AI zijn gebaseerd en onder toezicht van het Comité staan. Dit probleem, dat in het bijzonder aanwezig is bij agent-gebaseerde systemen, geldt voor elk AI-systeem. De schaalverandering in de gecontroleerde activiteit moet, indien nodig, vergezeld kunnen gaan van een schaalverandering in de controlemodaliteiten.

Het Comité beveelt daarom aan dat het ontwerp voorziet in de bevoegdheid om, bij gemotiveerde beslissing van het Comité, controlemodules op de AI-systemen te installeren. Aangezien elk systeem verschillend is, moet de technische oplossing voor de controlemodule te goeder trouw worden besproken tussen het Comité en de gecontroleerde dienst. Voorbeelden van mogelijke technieken zijn application programming interfaces (API's), 'trusted execution environments' (beveiligde uitvoeringsomgevingen) of 'sidecar'-modules. Wanneer commerciële oplossingen worden gebruikt, moeten de dienstenovereenkomsten of gebruikslicenties een clause bevatten die de private partner verplicht de installatie van toezichtsmodules door de toezichthoudende autoriteit te aanvaarden (ADV-17).

(4) PLEGEN VAN MISDRIJVEN

Overtredingen, GAS-inbreuken en Wegcode (art. 13/1 WIV)

23. M.b.t. art. 13/1 WIV stelt de memorie van toelichting²⁹: *“In artikel 13/1 worden verschillende wijzigingen aangebracht.*

Vooreerst wordt het toepassingsgebied van de tweede paragraaf van artikel 13/1 aangepast. Tot op heden konden agenten overtredingen, inbreuken op de wegcode en gebruiksdiefstal plegen indien dit strikt noodzakelijk is voor het wegslagen van de optimale uitvoering van de opdracht of ter verzekering van hun eigen veiligheid of die van derden. Deze strafbare feiten kunnen enkel worden gepleegd wanneer de agenten belast zijn met de uitvoering van de methoden voor het verzamelen van gegevens, ofwel wanneer de agenten leden zijn van het interventieteam. De wijziging beoogt de strafbare feiten die kunnen worden gepleegd door de agenten van de inlichtingen- en veiligheidsdiensten aan te passen in het licht van het nieuwe Strafwetboek.

*Zo worden GAS-inbreuken toegevoegd aan de mogelijk te plegen feiten. Deze kleine inbreuken doen zich in de praktijk namelijk voor in situaties waar de inlichtingen- en veiligheidsdiensten snel moeten kunnen handelen. Hoewel deze feiten een beperkte juridische zwaarte hebben, spelen deze steeds vaker een operationeel relevante rol.”*³⁰

24. Vooreerst merkt het Comité op dat in art. 13/1 het woord “overtredingen” niet werd geschrapt. Dit dient te geschieden (ADV-18) gezien het nieuwe Strafwetboek de bestaande overtredingen ofwel heeft afgeschaft ofwel heeft opgewaardeerd naar een misdrijf met strafniveau 1. Ingeval de opsteller wenst dat bepaalde van deze naar een misdrijf met strafniveau 1 opgewaardeerde overtredingen voor de toekomst eveneens voorwerp kunnen uitmaken van een strafuitsluitende verschoningsgrond, dienen betrokken wetsartikelen van het nieuwe Strafwetboek expliciet in art. 13/1 opgesomd te worden.

25. Ten tweede stelt het Comité vast dat voorgesteld wordt om het begrip “GAS-inbreuken” aan art. 13/1 WIV toe te voegen. Onmiddellijk dient opgemerkt te worden dat het Comité de memorie van toelichting niet volgt dat GAS-inbreuken louter kleine inbreuken zijn, met een beperkte juridische zwaarte. Doorheen de diverse aanpassingen van de GAS-wet en de Wegverkeerswet verkregen de gemeenten ook de bevoegdheid om bepaalde wanbedrijven te sanctioneren met een GAS-boete. Gelet op de strafmaat van wanbedrijven zijn dit geen kleine inbreuken.

²⁹ Memorie van toelichting, pag. 39-40.

³⁰ Eigen onderlijning van het Comité.



Daarnaast brengt het Comité onder de aandacht dat het woord “GAS-inbreuken” geen vastomlijnd wettelijk begrip is (i.t.t. het begrip gebruiksdiefstal die duidelijk verwijst naar art. 461, tweede lid SW-1867). Hierdoor is de loutere toevoeging van het begrip “GAS-inbreuken” aan art. 13/1 WIV niet afdoende. Er moet verduidelijkt worden voor welke inbreuken er exact een strafuitsluitende verschoningsgrond voor agenten wordt ingevoerd (ADV-19).

In dit kader lijkt ook art. 29, §2, tweede lid van de Wegverkeerswet van belang. Deze stelt: *“Het in voormelde reglementen omschreven parkeren met beperkte parkeertijd, betalend parkeren en parkeren op plaatsen voorbehouden aan houders van een gemeentelijke parkeerkaart worden niet strafrechtelijk bestraft, behoudens het half-maandelijks beurtelings parkeren, de beperking van het langdurig parkeren, en bedrog met de parkeerschijf.”*. Wegens de depenalisering van betrokken inbreuken betreffen het niet langer inbreuken van strafrechtelijke aard maar inbreuken van administratiefrechtelijke aard die gesanctioneerd kunnen worden met ofwel een bestuurlijke sanctie (een zgn. GAS-boete) ofwel een retributie. Het woord “straf” in huidig art. 13/1 lijkt hierdoor niet afdoende te zijn om laatstgenoemde reacties te dekken.

26. Ook in de ontwerpen van art. 19/3, §1 en 19/4 wordt het woord “GAS-inbreuken” gehanteerd, wat volgens het Comité derhalve een aanpassing behoeft (ADV-20).

27. Tot slot brengt het Comité in herinnering dat op 1 juni 2027 de Wegcode vervangen wordt door de federale Code van de openbare weg, de Brusselse Code van de openbare weg, het Vlaams Verkeersreglement en de Waalse Code van de openbare weg. Dit is van belang voor artikel 13/1, §1 WIV. In het licht van deze toekomstige wijziging en ter bevordering van de leesbaarheid van artikel 13/1, §1 WIV adviseert het Comité volgend definitie toe te voegen aan de lijst van begrippen in artikel 3 (ADV-21):

“Wegcode : de federale Code van de openbare weg, de Brusselse Code van de openbare weg, het Vlaams Verkeersreglement en de Waalse Code van de openbare weg;”

Een artikel op het einde van het wetsontwerp dient te worden toegevoegd waarbij de inwerkingtreding van deze bepaling gesteld wordt op 1 juni 2027.

Provocatieverbod

28. Aanvullend op het aspect plegen van misdrijven. Het Comité is van oordeel dat in hoofde van de personeelsleden van de inlichtingendiensten een wettelijk verbod tot provocatie van misdrijven dient te worden ingesteld (ADV-22) dat vergelijkbaar is met het wettelijk provocatieverbod ten aanzien van de politieambtenaren (art. 30 V.T.Sv.).

Artikel 30 V.T.Sv. stelt:

‘Provocatie van misdrijven is verboden.

Er is provocatie wanneer in hoofde van de dader het voornemen om een misdrijf te plegen rechtstreeks is ontstaan of versterkt, of is bevestigd terwijl hij dit wilde beëindigen, door de tussenkomst van een politieambtenaar, van een derde handelend op het uitdrukkelijk verzoek van deze ambtenaar of van een burgerinfiltrant in het kader van een burgerinfiltratie bedoeld in boek I, hoofdstuk IV, afdeling III onderafdeling 4bis van het Wetboek van strafvordering.

In geval van provocatie is de strafvordering onontvankelijk wat deze feiten betreft.’

Een dergelijk verbod kan zowel ingeschreven worden via een aanpassing van vernoemd artikel 30 V.T.Sv. alsook in de Inlichtingenwet (bv. in een toe te voegen §5 van art. 13 WIV). Omdat de Inlichtingenwet *de lege lata* een eigen regeling bevat voor het plegen van misdrijven door de inlichtingendiensten én omwille van de grotere zichtbaarheid voor de personeelsleden van de inlichtingendiensten die meer vertrouwd zijn met deze wet,



prefereert het Comité een aanvulling in de Inlichtingenwet. Vertrekkende vanuit artikel 30 V.T.Sv. – deze bepaling correspondeert immers met de rechtspraak van het Hof van Cassatie en het Grondwettelijk Hof voor wat betreft de betrokken definitie (tweede lid) en veruitwendigd de wil van de wetgever voor wat betreft de betrokken sanctie (derde lid) – wordt een dergelijk verbod best als volgt verwoord:

[Art. 13, §5]:

‘Provocatie van misdrijven is verboden.

Er is provocatie wanneer in hoofde van de dader het voornemen om een misdrijf te plegen rechtstreeks is ontstaan of versterkt, of is bevestigd terwijl hij dit wilde beëindigen, door de tussenkomst van een agent van een inlichtingen- en veiligheidsdienst of van een derde handelend op het uitdrukkelijk verzoek van dit personeelslid.

In geval van provocatie is de strafvordering onontvankelijk wat deze feiten betreft.’

29. Een dergelijk wettelijk verbod moet volgens het Comité om diverse redenen worden ingevoegd. Vooreerst herinnert het Comité eraan dat het wettelijk provocatieverbod ten aanzien van de politieambtenaren er reeds kwam middels de Wet Bijzondere Opsporingsmethoden van 6 januari 2003 (invoeging van een artikel 47^{quater} Sv). Na vernietiging door het Grondwettelijk Hof³¹ van artikel 47^{quater} Sv³² werd dit door de BOM-reparatiewet van 27 december 2005 ingevoegd in een nieuw artikel 30 V.T.Sv. Een kleine aanvulling vond plaats ten gevolge van de invoeging van een wettelijke regeling rond de burgerinfiltratie. Hoewel de BIM-wet van 4 februari 2010 voor de inlichtingendiensten vergelijkbare onderzoeksbevoegdheden als de BOM-methoden *sensu lato* creëerde, werd nagelaten om een vergelijkbaar verbod in te stellen rond de provocatie van misdrijven. Er bestaan evenwel geen inhoudelijk objectieve redenen waarom een dergelijk verbod zou dienen te gelden ten aanzien van de politieambtenaren doch niet ten aanzien van de agenten van de inlichtingendiensten. Een dergelijke vaststelling geldt heden des te meer nu vastgesteld kan worden dat de doelwitten van de inlichtingendiensten zich in toenemende mate bewegen binnen een criminele milieu. Dit heeft zowel te maken met de wil van de wetgever om bepaalde nationale veiligheidsdreigingen waarvoor de VSSE en de ADIV bevoegd zijn, via strafrechtelijke weg te bestrijden en aldus strafbaar te stellen, alsook met bepaalde feitelijke omstandigheden op zich.

Ten tweede herinnert het Comité eraan dat het in artikel 13/1, §1 WIV bestaande verbod om misdrijven te plegen niet afdoende is om een provocatieverbod te dekken. Een middel dat bij provocatie werd aangewend om het misdadig voornemen bij een persoon te doen ontstaan, versterken of bevestigen hoeft geen misdrijf te zijn. Het hoeft zelfs niet onwettig te zijn, een vals middel volstaat.

Ten derde is van betekenis dat de inlichtingendiensten steeds meer bevoegdheden verkrijgen die bij de uitoefening ervan een gevaar op provocatie met zich meebrengen. Meer in het bijzonder noodzaakt de toekenning van verregaande verstoringsbevoegdheden aan de inlichtingendiensten tot een expliciet wettelijk verbod van provocatie van misdrijven in hoofde van de personeelsleden van de inlichtingendiensten. Het gebruik van informanten als beïnvloedingsagenten binnen een verstoringsactie bijvoorbeeld mag niet ontaarden in de inzet van agenten-provocateurs. Hoewel er legitieme redenen kunnen zijn om de VSSE en de ADIV meer bevoegdheden toe te kennen bij het verstoren van ernstige dreigingen, bestaat er geen objectieve rechtvaardiging voor de provocatie van strafbare feiten in dit kader. Niet enkel zou dit strijdig zijn met artikel 6, eerste lid EVRM ingeval betrokkenen het voorwerp zouden uitmaken van vervolging, binnen een democratische rechtsstaat valt de provocatie van misdrijven eenvoudig weg niet te legitimeren. Om die redenen alleen al vraagt het Comité om duidelijk in de Inlichtingenwet bovenstaand provocatieverbod in te schrijven.

³¹ Grondwettelijk Hof, arrest nr. 202/2004 van 21 december 2004.

³² Het Hof ging niet akkoord met het verschil in de wettelijke definitie van provocatie al naargelang er al dan niet een bijzondere opsporingsmethode werd aangewend.



30. Tot slot herinnert het Comité aan het arrest nr. 202/2004 van 21 december 2004 van het Grondwettelijk Hof. Het Hof ging niet akkoord met het verschil in de wettelijke definitie van provocatie al naargelang er al dan niet een bijzondere opsporingsmethode werd aangewend. Hieruit moet afgeleid worden dat het begrip provocatie ook ten aanzien van de inlichtingendiensten een algemene draagwijdte dient te hebben en zich niet mag beperken tot de bijzondere inlichtingenmethoden. Om die reden stelt het Comité voor op bovenstaand, voorgestelde alinea toe te voegen in een toe te voegen paragraaf 5 van artikel 13 WIV.

Lacune binnen de strafprocedure

31. Het Comité wenst via deze weg eveneens een lacune binnen de strafprocedure onder de aandacht te brengen. Binnen de strafprocedure beschikt een rechter, buiten een beperkt geval (*infra*), niet over de mogelijkheid om de wettigheid van een conform art. 19 WIV³³ overgemaakte en in het strafdossier neergelegde niet-geclassificeerde nota van een inlichtingendienst na te gaan, waaronder de wettigheid van de informatiegaring die voorafging aan de redactie van een dergelijke nota.

De (bestaande) beperkte procedure vormt de zgn. “prejudiciële adviesprocedure” (cf. artt. 131bis, 189quater en 279bis Sv) waarbij een strafgerecht aan het Comité R/I de regelmatigheid kan vragen van de BIM-methoden die aanleiding gaven tot het opstellen van een zogenaamd “niet-geclassificeerd proces-verbaal” (cf. art. 19/1 WIV). Dit proces-verbaal wordt door de BIM-Commissie opgesteld wanneer er aanwijzingen van misdrijven naar boven kwamen via het gebruik van BIM-methoden. De prejudiciële adviesprocedure wordt echter in de praktijk weinig toegepast. De flux van de gegevens van de inlichtingendiensten naar het parket vindt slechts uitzonderlijk plaats via een dergelijk proces-verbaal. De meeste informatie wordt overgemaakt via een nota van het diensthoofd van de inlichtingendiensten naar het parket (gebaseerd op de ambtelijke aangifte cf. artikel 29 Sv of – in hoofdzaak – de algemene mededelingsbevoegdheid cf. artikel 19 WIV).

Het Comité is van oordeel dat het ontbreken van een bijzonder toezicht gedurende de strafprocedure op het inlichtingenonderzoek problematisch kan worden ingeval een strafdossier informatie van een inlichtingendienst bevat die ingewonnen werd via de onrechtmatige aanwending van gewone methoden (bv. gebruik makende van gewone methoden daar waar dit diende te geschieden via de BIM-procedure) of die onrechtmatige persoonsgegevensverwerking bevat (bv. een persoon kwalificeren als gevaarlijk hoewel dit niet ondersteund wordt door de nodige informatie). In het licht hiervan beveelt het Comité aan om de “prejudiciële adviesprocedure in strafzaken” te veralgemenen (ADV-23). Hierbij dienen dan de strafgerichten de mogelijkheid te hebben om het Comité te vatten en te bevragen rond de wettigheid van alle niet-geclassificeerde inlichtingen afkomstig van de inlichtingendiensten die werden overgemaakt op grond van artikel 19 van de wet van 30 november 1998 en die zich in het strafdossier bevinden.

(5) OPEN BRONNEN (ontwerp paragraaf 3 in art. 16/1 WIV)

32. Een derde paragraaf wordt aan art. 16/1 WIV toegevoegd:

“In het belang van de uitoefening van hun opdrachten kunnen de inlichtingen- en veiligheidsdiensten alle informatie en persoonsgegevens verwerken die via de voor het publiek toegankelijke plaatsen van de informatica- en communicatiesystemen gaan, met inbegrip van deze die zijn verkregen door het plegen van strafbare feiten, ongeacht of er formaliteiten moeten worden vervuld om er toegang toe te krijgen.”

³³ Deze bepaling bevat de algemene mededelingsbevoegdheid van de inlichtingendiensten.



Betrokken bepaling creëert een rechtsgrond “om gegevens te verwerken die toegankelijk zijn in open bronnen maar verkregen werden door middel van strafbare feiten (Leaks-DB, Darknet)”³⁴, bijvoorbeeld door een klokkenluider van een buitenlandse inlichtingendienst.

33. Het Comité stelt voor om volgende verbeteringen aan te brengen (ADV-24):

“De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, alle informatie en persoonsgegevens die worden doorgegeven via voor het publiek toegankelijke delen van informatica- en communicatiesystemen, met inbegrip van informatie en persoonsgegevens die zijn verkregen door het plegen door derden van strafbare feiten, inwinnen, registreren en verwerken ongeacht of er door de inlichtingen- en veiligheidsdiensten formaliteiten moeten worden vervuld om er toegang toe te verkrijgen.”

Het Comité stelt namelijk vast dat de huidige bepaling moeilijk begrijpbaar is en tot interpretatieproblemen kan leiden. Het Comité stelt bovenstaande verbetering voor. Het merendeel van de verbeteringen betreffen louter taalkundige verbeteringen in de Nederlandstalige versie van betrokken bepaling en aanpassingen in het licht de wijze waarop andere wetsartikelen rond de methoden worden omschrijven (m.n. aanhef van de bepaling).

Het woord “verwerken” wordt verduidelijkt als “inwinnen, registreren en verwerken”. De toevoeging van het begrip “inwinnen” maakt duidelijk dat het om een inlichtingenmethode gaat; het wetsontwerp plaats betrokken bepaling immers in de onderafdeling die de gewone inlichtingenmethoden regelt. De toevoeging van het begrip “registreren” verduidelijkt dat er tegelijkertijd een specifieke bewaringsbevoegdheid mee gepaard gaat. Stel dat een klokkenluider van een buitenlandse inlichtingendienst een omstandig document (*de iure* dus een gegevensbestand) op het internet plaats. In dergelijk geval gaat de VSSE en de ADIV dit bestand logischerwijs niet enkel zo spoedig mogelijk wensen in te winnen – de volgende dag kan het document immers reeds werden verwijderd – doch ook dit op een interne gegevensbank wensen op te nemen (“registreren”). In een daaropvolgende fase zal de inlichtingendienst moeten nagaan welke gegevens daadwerkelijk voor hun taakoefening relevant zijn, en enkel die gegevens mogen bewaard worden in de centrale gegevensbank. Het begrip “verwerken” blijft behouden, maar door het te plaatsen op de laatste plaats wordt veruitwendigd dat het een generieke invulling kent, zoals bedoeld in art. 26, 2° en 72, §1 van de Gegevensbeschermingswet van 30 juli 2018.

34. De opsteller van het ontwerp moet voorzien in een mechanisme dat de diensten in staat stelt artikel 2, §2 van de WIV – m.b.t. de verwerking van gegevens die beschermd worden door het beroepsgeheim van advocaten, artsen en journalisten – na te leven wanneer de in artikel 16/1 bedoelde gegevens worden verwerkt. Het Comité beveelt, bijvoorbeeld, aan om een maximale termijn vast te stellen binnen dewelke de dienst de gegevens die hij niet mag verwerken, moet wissen (ADV-25).

34bis. Inlichtingendiensten maken steeds vaker gebruik van commercieel verkrijgbare en publiek beschikbare data (de zgn. *commercially and publicly available data*) zonder de traditionele juridische waarborgen die gelden voor de klassieke collecte en de verwerking van gegevens. Via deze weg verkrijgen de diensten een groeiende hoeveelheid persoonsgegevens via databrokers, aangekochte datasets (ook uit datalekken), commerciële analysetools, open-source intelligence (OSINT) en vrijwillige gegevensoverdracht door private bedrijven. Inlichtingendiensten zijn daarom steeds minder afhankelijk van klassieke inlichtingenmethoden en maken steeds meer gebruik van commerciële databronnen. Omdat deze informatiegaring meestal niet-afgedwongen is, vallen deze inlichtingenactiviteiten vaak buiten enige externe controle. Hierdoor ontstaat een steeds belangrijker wordende blinde vlek binnen de democratische controle. Het Comité erkent dat het voor de VSSE en de ADIV in bepaalde gevallen en onder bepaalde omstandigheden nuttig kan zijn om (per-

³⁴ Memorie van toelichting, pag. 50.



soons)gegevens aan te kopen van databrokers. Tegelijkertijd stelt het Comité vast dat er actueel onvoldoende juridische waarborgen bestaan binnen deze vorm van informatiegaring en -verwerking. Het Comité beschikt actueel ook niet over de nodige juridische instrumenten om effectief en efficiënt een toezicht uit te oefenen op deze vorm van informatiegaring en -verwerking. Om deze reden adviseert het Comité om een duidelijk wettelijk kader te creëren rond de aankoop en verwerking van commerciële data (bv. een verplichte risicoanalyses rond privacy en andere grondrechten, verplichte compliance-processen, een verbod op bepaalde discriminerende toepassingen van aangekochte data), met een voorafgaande autorisatie voor risicovolle vormen van dataverzameling, en een onafhankelijk toezicht verricht door het Comité. Tevens dient er volgens het Comité een wettelijk verbod te komen dat inlichtingendiensten persoonsgegevens kopen waarvoor zij normaal een toestemming van de BIM-Commissie nodig hebben of een verplichting dat dergelijk persoonsgegevens slechts kunnen aangekocht worden mits een dergelijke voorafgaande toestemming. Tot slot pleit het Comité sterk om bindende beslissingen te kunnen nemen tot het verwijderen van datasets of tot de stopzetting van een aankoop bij een vastgestelde onwettigheid (ADV-25bis).

(6) TOEGANG TOT EU-DATABANKEN: EES (ontwerp art. 16/3/2 WIV), ETIAS EN EURODAC

35. Het Comité stelt vast dat het ontwerp van art. 16/3/2 WIV een toegangsrecht inricht tot het EES (Entry/Exit System)³⁵, het zgn. inreis- en uitreisstelsel van de EU voor het voorkomen, opsporen of onderzoeken van terroristische misdrijven en andere ernstige strafbare feiten.

Het Comité stelt eveneens vast dat het ontwerp art. 16/3/2 gebaseerd is op en quasi woordelijk overeenkomt met het huidige art. 16/3/1 dat een toegangsrecht inricht tot het ETIAS-systeem (European Travel Information and Authorisation System)³⁶.

Het Comité brengt in herinnering dat het recent een wetgevingsadvies³⁷ verleende rond de inrichting van een toegangsrecht voor de inlichtingendiensten tot Eurodac (European Asylum Dactyloscopy)³⁸. Dit is een centraal beheerde databank van de Europese Unie. Concreet wordt deze operationeel en technisch beheerd door het Europese Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). In vernoemd advies stelt het Comité: *"Het Comité staat positief tegenover een toegangsbevoegdheid voor de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichting en Veiligheid (ADIV), evenwel onder de voorwaarde dat in de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (WIV) de nodige voorwaarden en procedures worden toegevoegd die moeten worden*

³⁵ Verordening (EU) 2017/2226 van het Europees Parlement en de Raad van 30 november 2017 tot instelling van een inreis-uitreisstelsel (EES) voor de registratie van inreis- en uitreisgegevens en van gegevens over weigering van toegang ten aanzien van onderdanen van derde landen die de buitengrenzen overschrijden en tot vaststelling van de voorwaarden voor toegang tot het EES voor rechtshandavingsdoeleinden (...), PbEU 9 december 2017, L 327/20.

³⁶ Verordening (EU) 2018/1240 van het Europees Parlement en de Raad van 12 september 2018 tot oprichting van een Europees reisinformatie- en -autorisatiesysteem (Etias) (...), PbEU 19 september 2018, L 236/1.

³⁷ Advies nr. 2026/003 van 10 februari 2026 van het Comité R/I m.b.t. het 'wetsontwerp tot wijziging van de vreemdelingenwet: toegang tot Eurodac voor VSSE en ADIV' (www.comiteri.be).

³⁸ Verordening (EU) 2024/1358 van het Europees Parlement en de Raad van 14 mei 2024 betreffende de instelling van "Eurodac" voor de vergelijking van biometrische gegevens om de Verordeningen (EU) 2024/1351 en (EU) 2024/1350 van het Europees Parlement en de Raad en Richtlijn 2001/55/EG van de Raad doeltreffend toe te passen en om illegaal verblijvende onderdanen van derde landen en staatlozen te identificeren en betreffende verzoeken van rechtshandavingsinstanties van de lidstaten en Europol om vergelijkingen van Eurodac-gegevens ten behoeve van rechtshandaving, tot wijziging van de Verordeningen (EU) 2018/1240 en (EU) 2019/818 van het Europees Parlement en de Raad en tot intrekking van Verordening (EU) nr. 603/2013 van het Europees Parlement en de Raad, PbEU L van 22.05.2024.



gevolgd bij de uitoefening van deze bevoegdheid. Eurodac bevat immers gevoelige persoonsgegevens, meer bepaald biometrische gegevens (vingerafdruk, gezichtsopname). Het uitoefenen van een dergelijke toegangsbevoegdheid door de VSSE en de ADIV noodzaakt eveneens tot een verhoogd extern toezicht.”.

36. Omdat EES, ETIAS en EURODAC drie EU-databanken zijn, omdat in het voorliggend wetsontwerp de opsteller zelf de duidelijke wil veruitwendigd om EES en ETIAS aan eenzelfde procedure te onderwerpen indachtig dat het ontwerp art. 16/3/2 dezelfde procedure bevat dat het huidige art. 16/3/1 en gelet op voornoemde advies van het Comité (*supra*), is het Comité van oordeel dat het huidige artikel 16/3/1 WIV – dat heden de toegang regelt tot het ETIAS-systeem – best wordt vervangen en veralgemeend (ADV-26) zoals hierna-volgend verduidelijkt (in vet gedrukt staan de wijzigingen en toevoegingen ten aanzien van het huidige artikel; een nadere toelichting hiervan volgt).

De algemene doelstelling van een nieuw artikel 16/3/1 WIV is om op algemene wijze de materiële en formele voorwaarden te bepalen die van toepassing zijn bij de uitoefening van een toegangsrecht door de VSSE en de ADIV tot een centraal beheerde³⁹ EU-databank waar de inlichtingendiensten over een toegangsrecht beschikken, en die vergelijkbare intrusieve persoonsgegevens bevatten. Hierbij worden wel een aantal wijzigingen aan het huidige artikel 16/3/1 WIV gebracht – en bijgevolg ook aan het ontwerp van art. 16/3/2 WIV – die volgens het Comité noodzakelijk zijn in het licht van een onafhankelijke controle.

Artikel 16/3/1.⁴⁰

³⁹ Dus bijvoorbeeld niet bij een toegang tot PNR-gegevens, zoals geregeld in artikel 16/3 WIV.

⁴⁰ Huidig artikel 16/3/1 stelt:

§ 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, mits afdoende motivering, beslissen om toegang te hebben tot de gegevens opgeslagen in het centrale Etias-systeem overeenkomstig artikel 13 van de wet van 29 maart 2024 betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E.).

§ 2. Met uitzondering van de in paragrafen 4 en 5 bedoelde gevallen, kan de in paragraaf 1 bedoelde methode slechts worden aangewend nadat de voorzitter van de Commissie, of een ander lid indien de voorzitter niet onmiddellijk beschikbaar is, een voorafgaande controle heeft uitgevoerd van de schriftelijke en met redenen omklede beslissing van het betrokken diensthoofd of zijn gedelegeerde.

De beslissing van het betrokken diensthoofd of zijn gedelegeerde vermeldt:

1° de natuurlijke personen die het voorwerp uitmaken van de methode;

2° de feitelijke omstandigheden die de methode rechtvaardigen en de motivering inzake noodzakelijkheid en proportionaliteit;

3° de afdoende met redenen omklede aanduiding van het directe verband tussen de opdrachten bedoeld in de artikelen 7, 8 en 11 van deze wet en de doeleinden vermeld in artikel 13, § 1, van de wet van 29 maart 2024 betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E.);

4° in voorkomend geval, de redenen die de hoogdringendheid rechtvaardigen;

5° in voorkomend geval, de rechtvaardiging van de noodzakelijkheid om bepaalde gegevens van het centrale Etias-systeem te raadplegen.

De in het tweede lid bedoelde vermeldingen zijn op straffe van onwettigheid voorgeschreven.

§ 3. De voorzitter van de Commissie, of een ander lid indien de voorzitter niet onmiddellijk beschikbaar is, brengt aan het betrokken diensthoofd of zijn gedelegeerde een schriftelijk antwoord uit ten laatste de eerste werkdag na ontvangst van de in paragraaf 2 bedoelde beslissing.

De Commissie zendt alle documenten bedoeld in de paragrafen 2 en 3 onverwijld over aan het Vast Comité I.

§ 4. Indien de voorzitter van de Commissie, of een ander lid indien de voorzitter niet onmiddellijk beschikbaar is, een schriftelijk negatief antwoord uitbrengt of nalaat een schriftelijk antwoord uit te brengen binnen de termijn bedoeld in paragraaf 3, eerste lid, kan het betrokken diensthoofd, of zijn gedelegeerde, het Vast Comité I vatten, dat zo spoedig mogelijk antwoord zal geven om de methode voor het verzamelen van gegevens aan te wenden. Het Vast Comité I deelt zijn antwoord mee aan het betrokken diensthoofd of zijn gedelegeerde en aan de Commissie.

§ 5. In dringende gevallen, wanneer een dreigend gevaar voor het leven van een persoon moet worden voorkomen, kan het betrokken diensthoofd of zijn gedelegeerde de methode mondeling toestaan nadat hij een mondeling positief antwoord



“§ 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, mits afdoende motivering, beslissen om toegang te hebben tot de gegevens opgeslagen in de centraal beheerde EU-databanken waar de inlichtingen- en veiligheidsdiensten over een toegangsrecht beschikken, waaronder:

- het Etias-systeem overeenkomstig artikel 13 van de wet van 29 maart 2024 betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E.)

- het Eurodac-systeem overeenkomstig artikel 8septies, §2, eerste lid, 2° en 3° van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen

- het EES-systeem overeenkomstig artikel 2/2, §1, tweede lid van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen.

§ 2. Met uitzondering van de in paragrafen 4 en 5 bedoelde gevallen, kan de in paragraaf 1 bedoelde methode slechts worden aangewend nadat de voorzitter van de Commissie, of een ander lid indien de voorzitter niet onmiddellijk beschikbaar is, een voorafgaande controle heeft uitgevoerd van de schriftelijke en met redenen omklede beslissing van het betrokken diensthoofd of zijn gedelegeerde. De voorafgaande controle omvat een nazicht van de aanwezigheid van alle wettelijke vereisten om betrokken gegevens in te winnen.

De beslissing van het betrokken diensthoofd of zijn gedelegeerde vermeldt:

1° de natuurlijke personen die het voorwerp uitmaken van de methode;

2° de feitelijke omstandigheden die de methode rechtvaardigen en de motivering inzake noodzakelijkheid en proportionaliteit;

3° de afdoende met redenen omklede aanduiding van het directe verband tussen de opdrachten bedoeld in de artikelen 7 en 11 van deze wet en de geldende doeleinden vermeld in de toepasselijke Europese en nationale wetgeving;

4° in voorkomend geval, de redenen die de hoogdringendheid rechtvaardigen;

5° in voorkomend geval, de rechtvaardiging van de noodzakelijkheid om bepaalde gegevens van de betrokken centrale EU-databank te raadplegen.

De in het tweede lid bedoelde vermeldingen zijn op straffe van onwettigheid voorgeschreven.

§ 3. De voorzitter van de Commissie, of een ander lid indien de voorzitter niet onmiddellijk beschikbaar is, brengt aan het betrokken diensthoofd of zijn gedelegeerde een schriftelijk antwoord uit ten laatste de eerste werkdag na ontvangst van de in paragraaf 2 bedoelde beslissing.

De Commissie zendt alle documenten bedoeld in de paragrafen 2 en 3 onverwijld over aan het Vast Comité I.

heeft verkregen van de voorzitter van de Commissie, of een ander lid indien de voorzitter niet onmiddellijk beschikbaar is. Deze mondelinge beslissing wordt bevestigd door een met redenen omklede schriftelijke beslissing die de vermeldingen bedoeld in paragraaf 2 bevat, en die uiterlijk de eerste werkdag volgend op de datum van de mondelinge beslissing moet toekomen op de zetel van de Commissie.

§ 6. Zodra de beslissing van het betrokken diensthoofd of zijn gedelegeerde schriftelijk goedgekeurd wordt door de Commissie of het Vast Comité I, worden de elementen die noodzakelijk zijn voor de controle die uitgevoerd moet worden krachtens artikel 14, § 1, van de wet van 29 maart 2024 betreffende de oprichting en de organisatie van de opdrachten van de ETIAS Nationale Eenheid (E.N.E.), schriftelijk of op elektronische wijze overgezonden aan het centraal toegangspunt.

§ 7. De Commissie en het Vast Comité I kunnen op elk ogenblik controle uitoefenen op de wettigheid van de methode voor het verzamelen van gegevens, hierbij inbegrepen de in artikel 13 bepaalde principes, en de inlichtingen- en veiligheidsdiensten verbieden deze gegevens, verkregen in omstandigheden die de vigerende wettelijke bepalingen niet naleven, te exploiteren.

Wanneer het Vast Comité I vaststelt dat de gegevens werden verzameld in omstandigheden die de vigerende wettelijke bepalingen niet naleven, beveelt het de vernietiging ervan. In dat geval wordt het centraal toegangspunt hiervan op de hoogte gehouden.



§ 4. Indien de voorzitter van de Commissie, of een ander lid indien de voorzitter niet onmiddellijk beschikbaar is, een schriftelijk negatief antwoord uitbrengt of nalaat een schriftelijk antwoord uit te brengen binnen de termijn bedoeld in paragraaf 3, eerste lid, kan het betrokken diensthoofd, of zijn gedelegeerde, het Vast Comité I vatten, dat zo spoedig mogelijk antwoord zal geven om de methode voor het verzamelen van gegevens aan te wenden. Het Vast Comité I deelt zijn antwoord mee aan het betrokken diensthoofd of zijn gedelegeerde en aan de Commissie. Tegen de beslissing van het Comité is geen beroep mogelijk.

§ 5. In dringende gevallen, wanneer een dreigend gevaar voor het leven van een persoon moet worden voorkomen, kan het betrokken diensthoofd of zijn gedelegeerde de methode mondeling toestaan nadat hij een mondeling positief antwoord heeft verkregen van de voorzitter van de Commissie, of een ander lid indien de voorzitter niet onmiddellijk beschikbaar is. Deze mondelinge beslissing wordt bevestigd door een met redenen omklede schriftelijke beslissing die de vermeldingen bedoeld in paragraaf 2 bevat, en die uiterlijk de eerste werkdag volgend op de datum van de mondelinge beslissing moet toekomen op de zetel van de Commissie.

§ 6. Zodra de beslissing van het betrokken diensthoofd of zijn gedelegeerde schriftelijk goedgekeurd wordt door de Commissie of het Vast Comité I, wordt een schrijven van het diensthoofd of zijn gedelegeerde met de gevorderde gegevens, schriftelijk of op elektronische wijze overgezonden aan het betrokken nationaal/centraal toegangspunt. Dit schrijven maakt melding van de voorafgaande goedkeuring van de Commissie of het Vast Comité I.

§ 7. De Commissie en het Vast Comité I kunnen op elk ogenblik controle uitoefenen op de wettigheid van de methode voor het verzamelen van gegevens, hierbij inbegrepen de in artikel 13 bepaalde principes, en de inlichtingen- en veiligheidsdiensten verbieden deze gegevens, verkregen in omstandigheden die de vigerende wettelijke bepalingen niet naleven, te exploiteren.

Wanneer het Vast Comité I vaststelt dat de gegevens werden verzameld in omstandigheden die de vigerende wettelijke bepalingen niet naleven, beveelt het de vernietiging ervan. In dat geval wordt het nationaal/centraal toegangspunt hiervan op de hoogte gehouden.”.

37. Het Comité hanteert het huidige artikel 16/3/1 WIV als vertrekbasis om meerdere redenen.

Zoals gezegd, bevat het huidige artikel de regeling rond de toegangsbevoegdheid van de VSSE en de ADIV tot de zgn. ETIAS-gegevens (European Travel Information and Authorisation System, oftewel de reisinformatie van onderdanen van visumvrije landen). ETIAS en Eurodac zijn vergelijkbaar indachtig de gelijkaardige aard van de toegankelijke gegevens en de gelijkmatige omvang van inmenging in de persoonlijke levenssfeer.

Het Comité stelt vast dat de inlichtingendiensten actueel niet worden opgesomd in art. 2/2 Vreemdelingenwet en bijgevolg geen toegangsrecht hebben tot de EES-databank. In betrokken bepaling geeft de wetgever de Koning de bevoegdheid om andere overheidsinstellingen een dergelijk toegangsrecht te geven. Het Comité stelt vast dat EES, net zoals Eurodac en ETIAS, een centrale EU-databank is die gegevens bevat met een gelijkmatige omvang in de persoonlijke levenssfeer. Een desgevallend door de Koning ingericht toegangsrecht voor de inlichtingendiensten zou volgens het Comité dus eveneens niet kunnen geschieden zonder dat de wetgever vergelijkbare materiële en formele voorwaarden bepaalt.

Net zoals de Wet van 16 mei 2024⁴¹ die het actuele artikel 16/3 WIV invoerde die het toegangsrecht van de inlichtingendiensten regelt tot de passagiersgegevens zoals bedoeld in artikel 27 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens, werd bij de Wet van 29 maart 2024⁴² die het actuele artikel 16/3/1 WIV invoerde, vertrokken vanuit de redenen waarom het Grondwettelijk Hof een eerdere versie

⁴¹ Wet 16 mei 2024 tot wijziging van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens.

⁴² Wet 29 maart 2024 betreffende de oprichting en de organisatie van de opdrachten van ETIAS Nationale Eenheid (E.N.E.).



van artikel 16/3 van de Wet van 30 november 1998 had geannuleerd (zie arrest nr. 131/2023 van 12 oktober 2023). Centraal in de argumentatie van het Hof staat dat een toegang tot betrokken databank mogelijk is doch onder de strikte voorwaarde van een voorafgaand akkoord van een rechterlijke of onafhankelijk controle-instantie. In de artt. 16/3 en 16/3/1 werd deze bevoegdheid – voor wat betreft de VSSE en de ADIV – toegekend aan de BIM-Commissie. Bij uitblijven van een akkoord van de BIM-Commissie of in beroep dient een voorafgaand akkoord gevraagd te worden van het Comité R/I.

38. Volgende wijzigingen aan het huidige artikel 16/3/1 WIV – en bijgevolg ook aan het ontwerp van art. 16/3/2 WIV – zijn volgens het Comité evenwel noodzakelijk.

Een eerste belangrijke wijziging werd aangebracht in paragraaf 6. Deze paragraaf doet namelijk afbreuk aan de systematiek van de externe wettigheidscontrole op inlichtingenmethoden geregeld in de Wet van 30 november 1998. Zoals hierboven verduidelijkt, is het de taak van de BIM-Commissie en desgevallend het Comité R/I om een wettigheidscontrole uit te voeren op het ontwerp van beslissing om betrokken gegevens in te winnen (m.n. Eurodac-gegevens, ETIAS-gegevens, EES-gegevens). Eenmaal als wettig beoordeeld komt het niet toe aan een externe administratieve overheid (m.n. de geïntegreerde politie m.b.t. de Eurodac-gegevens⁴³; de dienst ETIAS van het NTTC bij het Nationale Crisiscentrum m.b.t. ETIAS-gegevens) om deze beoordeling te overrulen.

Zoals betrokken bepaling verduidelijkt, komt het Comité R/I in deze procedure tussen bij uitblijven van een beslissing van de BIM-Commissie of in graad van beroep. Een beslissing van het Comité ter zake is jurisdictioneel van aard. Een overruling van de geïntegreerde politie zou neerkomen – en komt neer, voor wat betreft de tussenkomst van het NTTC bij het inwinnen van ETIAS-gegevens – op een administratieve beslissing die een gerechtelijke beslissing aan de kant schuift, en dit binnen een wettigheidscontrole.⁴⁴ Het Comité dringt daarom sterk aan om de huidige paragraaf 6 te herzien (ADV-27).

In paragraaf 2 wordt de taak van de BIM-Commissie, desgevallend van het Comité R/I verduidelijkt zoals actueel reeds van toepassing. Een wettigheidscontrole omvat nazicht van alle wettelijk vereisten om betrokken gegevens in te winnen, zowel degene in de Wet van 30 november 1998 alsook de specifieke toepassingsvoorwaarden opgenomen in nationale en Europese regels.

In paragraaf 6 wordt verder verduidelijkt dat tegen een beslissing van het Comité geen beroep mogelijk is. Eenmaal het Comité jurisdictioneel heeft vastgesteld dat het ontwerp van beslissing van het diensthoofd of zijn gedelegeerde wettig is, kan het, zoals verduidelijkt, niet zijn dat een externe administratieve overheid anders beslist. Deze bepaling is gebaseerd op artikel 43/8 van de Wet van 30 november 1998.

⁴³ Ook de Gegevensbeschermingscommissie (GBA) stelt dat de geïntegreerde politie niet aangewezen is als controlerende autoriteit. Meer bepaald stelt de GBA: *“De aanwijzing van de geïntegreerde politie voldoet niet aan de vereisten van onafhankelijkheid en onpartijdigheid (waaronder met name het ontbreken van een belangenconflict met de operationele eenheden die de verzoeken om toegang tot Eurodac zullen indienen), zoals vereist door artikel 6 van de Eurodac-verordening (...)”*. Advies nr. 47/2026 van 17 maart 2026 met betrekking tot het voorontwerp van wet tot wijziging van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen ter uitvoering van het Migratie- en asielpact van de Europese Unie (CO-A-2025-219), pag. 14, 17, 18 en 36. Dit advies werd gepubliceerd op de website van de Kamer als *Parl. St.* Kamer 2025-2026, nr. 56-1401/002.

⁴⁴ Het Comité is om die reden van oordeel dat de huidige paragraaf 6 van art. 16/3/1 WIV ongrondwettig is.



(7) NIET-PRIVACYGEVOELIGE BEELDEN (ontwerp art. 16/7 WIV)

39. Er wordt een nieuw art. 16/7 WIV ingevoegd:

Eerste lid: *“In afwijking van de artikelen 18/4 en 18/11 mogen de inlichtingen- en veiligheidsdiensten, in het belang van de uitoefening van hun opdrachten, vaste of bewegende beelden opnemen, op voorwaarde dat deze beelden op zichzelf niet voldoende zijn om een natuurlijke persoon te identificeren.”*

De memorie van toelichting verduidelijkt: *“Het huidige ontwerp introduceert een nieuwe gewone methode om de inlichtingen- en veiligheidsdiensten in staat te stellen vaste of bewegende beelden te maken van strategische locaties, zoals militaire, industriële of transportinfrastructuur, zonder gebruik te maken van de specifieke of uitzonderlijke methoden die in de organieke wet zijn voorzien. Deze aanpak is gerechtvaardigd vanwege het ontbreken van een schending van de privacy wanneer deze beelden op zichzelf geen natuurlijke personen identificeren, met als doel het toezicht op zones of faciliteiten en niet op individuen. Snelle toegang tot deze beelden, met name satellietbeelden, is essentieel om dreigingen te anticiperen, operaties te ondersteunen of te reageren op noodsituaties, zoals geïllustreerd door de achtervolging van Jürgen Conings of het beheer van de overstromingen van 2021. De introductie van deze gewone methode zal de inlichtingendiensten en veiligheidsdiensten in staat stellen hun operationele efficiëntie te versterken, terwijl de naleving van de fundamentele rechten van natuurlijke personen wordt gewaarborgd.”*⁴⁵

40. Deze bepaling werpt verschillende problemen op. Ten eerste moet het territoriale toepassingsgebied van de methode worden gepreciseerd. Enerzijds maakt ze niet duidelijk of de VSSE deze buiten het grondgebied kan inzetten, maar vanaf dit grondgebied (bijvoorbeeld door het besturen van een drone of een satelliet). De nieuwe gewone methode is immers gecreëerd met verwijzing naar de specifieke en uitzonderlijke methoden waarin de artikelen 18/4 en 18/11 voorzien. Deze laatste methoden kunnen door de VSSE worden ingezet bij de uitoefening van bepaalde opdrachten *“op of vanaf het grondgebied van het Koninkrijk”*. Wat de ADIV betreft, stelt het Comité I vast dat deze nieuwe methode de eigen bevoegdheid van de ADIV voor het maken van afbeeldingen in het buitenland (art. 44/2 WIV) gedeeltelijk uitholt. Deze laatste bepaling zal uitsluitend van toepassing blijven op afbeeldingen die in het buitenland zijn gemaakt en die op zichzelf de identificatie van een natuurlijke persoon mogelijk maken. Maar voor afbeeldingen die in België of in het buitenland zijn gemaakt en die op zichzelf geen identificatie mogelijk maken, zal artikel 16/7 van toepassing zijn. De aandacht van de wetgever wordt op dit feit gevestigd. Het Comité beveelt aan dit punt te verduidelijken (ADV-28).

41. Ten tweede is het criterium van de mogelijke identificatie van een natuurlijke persoon door de afbeeldingen zelf dubbelzinnig en onuitvoerbaar. Een afbeelding wordt immers altijd gebruikt in een context en in samenhang met andere gegevens. Het in de memorie van toelichting gekozen voorbeeld van de zoektocht naar Jürgen Conings is juist een merkwaardig voorbeeld van afbeeldingen die het niet mogelijk maken om iemand te identificeren: door luchtbeelden te maken van de bossen waar naar hem werd gezocht, was het doel immers juist om hem met een zekere precisie te kunnen identificeren. Men mag veronderstellen dat de onderzoekers zochten naar een geïsoleerd individu op de vlucht, eerder dan naar een grote groep wandelaars met dieren of een groep fietsende kinderen. Evenzo maakt het maken van satellietbeelden met een lage resolutie het ook mogelijk om individuen te identificeren. Als een voertuig regelmatig voor een huis wordt opgemerkt, of als men weet dat het aan een bepaald individu toebehoort, is de aanwezigheid van dit voertuig op een andere plaats een goede aanwijzing dat de betrokkene zich daar bevindt. Door deductie heeft men de persoon geïdentificeerd, zelfs als de afbeelding op zich dit niet mogelijk maakt. Men begrijpt dus dat een afbeelding altijd in een context wordt geplaatst, gekruist wordt met gegevens of vergeleken wordt met een afbeelding van een geïdentificeerde persoon, maar dat zij op zich slechts zelden

⁴⁵ Memorie van toelichting, pag. 15.



"op zichzelf" toelaat om een persoon te identificeren. Aangezien de identificatie van een persoon (in voorkomend geval op waarschijnlijke wijze) afhangt van de context en van andere gegevens, lijkt het voor het Comité onmogelijk om vooraf te weten of een afbeelding het mogelijk zal maken om een individu te identificeren. Het Comité verzet zich er op zich niet tegen dat bepaalde beeldopnamen onder de regeling van het ontworpen artikel 16/7 vallen, maar beveelt aan het essentiële criterium ervan te verduidelijken.

Samenvattend, het Comité brengt onder de aandacht dat conform het gegevensbeschermingsrecht er reeds sprake is van persoonsgegevens van zodra een natuurlijk persoon *identificeerbaar* is. Vaak zijn beelden die "*op zichzelf niet voldoende zijn om een natuurlijke persoon te identificeren*" wel reeds persoonsgegevens (bv. beelden van een groep betogers), en is bijgevolg "*het opnemen*" van dergelijke beelden wel reeds een verwerking van persoonsgegevens en mogen zij niet vervat liggen in deze nieuwe laagdrempelige bevoegdheid. In het licht van deze overweging dringt het Comité aan op een tekstuele wijziging in het wetsontwerp. Overeenkomstig de andere artikelen van de Inlichtingenwet stelt het Comité daarnaast voor om, in de Nederlandstalige tekst, het woord "mogen" te vervangen door "kunnen" (ADV-29).

42. Tweede lid:

"Beide inlichtingen- en veiligheidsdiensten houden een register bij van de beeldopnames gemaakt overeenkomstig het vorige lid. De betrokken inlichtingen- en veiligheidsdienst maakt maandelijks een lijst van de gemaakte beeldopnames over aan het Vast Comité I. Het Vast Comité I verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de beeldopnames gemaakt in omstandigheden die niet aan de wettelijke bepalingen voldoen."

Net zoals voorzien in art. 16/3, §7 en art. 16/3/1, §7 en het ontwerp van art. 16/3/2, §7 stelt het Comité voor om volgende zin toe te voegen (ADV-30): "*Wanneer het Vast Comité I vaststelt dat de gegevens werden verzameld in omstandigheden die de vigerende wettelijke bepalingen niet naleven, beveelt het hun vernietiging.*".

43. Voorts stelt het Comité voor om betrokken zin eveneens toe te voegen in de vergelijkbare bepalingen – art. 16/4, §2, vierde lid, en §3, vierde lid, en art. 16/6, §3 (ADV-31) – waar eveneens een bevoegdheid voor het Comité tot het verstrekken van een exploitatieverbod werd ingesteld doch waar eerder wetgevend werk de toevoeging van het bijbehorend vernietigingsbevel werd vergeten.

(8) INZET VAN INLICHTINGENMETHODEN OMWILLE VAN VEILIGHEIDSREDENEN (nieuw art. 18/1 WIV)

44. Er wordt een nieuw art. 18/1 WIV ingevoegd:

Eerste lid: "*In het belang van de uitoefening van hun opdrachten bedoeld in de artikelen 7, 1° en 3° /1 en 11, § 1, 1° tot 3° en 5°, kunnen de inlichtingen- en veiligheidsdiensten de methoden voor het verzamelen van gegevens aanwenden teneinde de veiligheid van hun agenten en van de uitvoering van hun opdrachten te verzekeren.*".

Overeenkomstig de andere artikelen van de Inlichtingenwet stelt het Comité voor om, in de Nederlandstalige tekst, de structuur van het begin van de alinea te veranderen in (ADV-32): "*De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten bedoeld in de artikelen 7, 1° en 3° /1 en 11, § 1, 1° tot 3° en 5°, de (...)*".

45. Het Comité stelt vast dat betrokken wetsbepaling de mogelijkheid creëert om alle gewone, specifieke en uitzonderlijke inlichtingenmethoden te kunnen inzetten omwille van veiligheidsredenen, meer bepaald teneinde de veiligheid van de agenten van de betrokken inlichtingen- en veiligheidsdienst of de veiligheid van de taakuitvoering te verzekeren. Nergens in de memorie van toelichting wordt echter een rechtvaardiging en



motivatie gegeven waarom een bepaalde methode voor dit doel noodzakelijk is. In het licht hiervan is het Comité van oordeel dat in de memorie van toelichting voor alle inlichtingenmethoden een motivatie moet worden gegeven waarom een bepaalde methode voor dit doel noodzakelijk is. Indien slechts voor welbepaalde methoden een motivatie kan gevonden worden, moet de wetsbepaling het toepassingsgebied tot de inzet voor die methoden beperken (ADV-33).

46. Omdat betrokken bepaling geen inlichtingenmethode bevat doch enkel het toepassingsgebied voor een geheel van methoden, is het Comité van oordeel dat het wetsontwerp betrokken bepaling op de verkeerde plaats in de Inlichtingenwet invoegt. Momenteel staat deze bepaling onder de onderafdeling die de gewone methoden regelt. Zoals gezegd, regelt deze bepaling echter geen gewone methode. De motivatie van deze plaats in de memorie van toelichting overtuigt bijgevolg niet. Veeleer hoort deze wetsbepaling thuis in de onderafdeling algemene bepalingen; dus net na het huidige art. 12 WIV.

Daarenboven, omwille van de invoeging van een nieuw art. 18/1 wordt het huidige art. 18/1 hernummers naar art. 18/2, en wordt het huidige art. 18/2 hernummerd naar art. 18/2/1. Een verhuis van het voorgestelde art. 18/1 naar een bepaling net na het huidige art. 12 WIV zou ook tegemoet komen aan de legistische richtlijnen van de Raad van State. In zijn handleiding voor het opstellen van wetgevende en reglementaire teksten raadt de Raad van State ten stelligste af om de artikelen van een wettekst te vernummen naar aanleiding van de invoeging van een of meerdere artikelen tussen reeds bestaande artikelen.⁴⁶

Een van de belangrijkste redenen hiervoor is dat de bestaande interne of externe verwijzingen naar de vernummerde tekstonderdelen collectief fout worden, wat aanleiding kan geven tot misverstanden en vergissingen (Zie J. Van Nieuwenhove, *Handboek wetgeving. Theorie en praktijk van het wetgevingsbedrijf*, Brugge, die Keure, 2025, p. 302-304). Het wetsontwerp bevat inderdaad aanpassingen in diverse interne verwijzingen.

Dit geheel noodzaakt om het voorgesteld art. 18/1 te verplaatsen naar een bepaling na art. 12 WIV in het onderdeel algemene bepalingen (ADV-34).⁴⁷

47. Tweede lid: *“Onverminderd artikel 13, § 4, worden de persoonsgegevens die verzameld werden aan de hand van een in het eerste lid bedoelde methode vernietigd zodra het hoofd van de betrokken dienst of zijn gedelegeerde meent dat er geen gevaar meer bestaat voor de veiligheid van de agenten of een nadeel voor de uitvoering van de opdrachten.”.*

Het Comité adviseert, naast een verhuis van betrokken bepaling zoals boven beschreven, om na de woorden *“Onverminderd artikel 13, §4,”* de woorden “en artikel 29 van het Wetboek van strafvordering” toe te voegen (ADV-35). Eerstgenoemde woorden bevestigen de meldingsplicht van dreigingsgerelateerde informatie beschreven in artikel 13, §4 WIV in het kader van betrokken gewone inlichtingenmethode. Het Comité ondersteunt deze bevestiging doch brengt in herinnering dat betrokken informatie ook misdrijfgerelateerde informatie kan bevatten die bijgevolg relevant kan zijn voor het Openbaar Ministerie.

48. Ten tweede adviseert het Comité om, aanvullend, een maximumbewaartermijn van een jaar in te voegen in voorliggende bepaling (ADV-36).

⁴⁶ Raad van State, *Beginselen van de wetgevingstechniek. Handleiding voor het opstellen van wetgevende en reglementaire teksten*, 2008, p. 82-83 [beschikbaar op de website van de Raad van State: https://www.raadvst-consetat.be/?page=technique_legislative&lang=nl].

⁴⁷ En, in dit kader, het deel over AI te hernummeren te beginnen met een nieuw art. 12/2, die eveneens best wordt ondergebracht onder een eigen titel.



(9) PROCEDURE UITZONDERLIJKE METHODEN

Startpunt maximumduur (ontwerp art. 18/10, §1, tweede lid)

49. Het actuele art. 18/10, §1, tweede lid stelt:

“Behoudens andersluidende wettelijke bepaling mag de periode tijdens welke de uitzonderlijke methode voor het verzamelen van gegevens aangewend mag worden niet langer duren dan twee maanden, te rekenen vanaf de machtiging, onverminderd de mogelijkheid om de methode te verlengen overeenkomstig § 5.”.

Het wetsontwerp vervangt deze bepaling door:

“Behoudens andersluidende wettelijke bepaling kan de uitzonderlijke methode voor het verzamelen van gegevens slechts aangewend worden na de machtiging en mag deze niet langer duren dan twee maanden, onverminderd de mogelijkheid om de methode te verlengen overeenkomstig § 5.”.

De memorie van toelichting motiveert deze wijziging als volgt: “(...) dit artikel (verduidelijkt) (...) het startpunt van de maximale periode⁴⁸ tijdens welke de uitzonderlijke methode voor het verzamelen van gegevens mag worden aangewend. Het gaat om een analogie met de procedure voor specifieke methoden, waarbij wordt gestreefd naar een grotere coherentie en uniformiteit binnen het juridische kader. De geldende maximumtermijn wordt hierbij niet gewijzigd.”.⁴⁹

Het Comité stelt vast dat – in tegenstelling tot hetgeen de memorie van toelichting beweert – het voorgesteld artikel het startpunt van de maximumtermijn schrapt.

Ook stelt de voorgestelde bepaling dat er redenen kunnen zijn om een uitzonderlijke methode uit te voeren zonder machtiging. In het huidige artikel slaan de woorden “Behoudens andersluidende wettelijke bepaling” op de maximumduur van twee maanden (m.n. dat deze uitzonderlijk en ad hoc langer kan zijn; zoals het geval is in bv. art. 18/13 WIV: het gebruik van een frontstore voor informatiegarage). In het voorgestelde artikel slaan deze woorden echter op het hebben van een machtiging *an sich* om een uitzonderlijke methode te mogen aanwenden. Er bestaan in de Inlichtingenwet geen dergelijke uitzonderingen. Er is altijd een voorafgaand akkoord vereist, ofwel van de BIM-Commissie in plenaire vergadering, ofwel door de voorzitter (of een commissielid) van de BIM-Commissie, ofwel door de betrokken voorgedijminister.

In het licht van deze bemerkingen is het Comité van oordeel dat betrokken wijziging in zijn geheel dient te worden geschrapt (ADV-37).

50. In art. 18/10, §2, eerste lid WIV – dat de verplichte vermeldingen in een (ontwerp van) machtiging opsomt – wordt in punt 5° “de periode waarin de uitzonderlijke methode voor het verzamelen van gegevens kan worden aangewend, te rekenen vanaf de machtiging van het diensthoofd” de woorden “te rekenen vanaf de machtiging van het diensthoofd” geschrapt.

In het licht van boven beschreven bemerkingen is het Comité van oordeel dat betrokken wijziging in zijn geheel dient te worden geschrapt (ADV-38).

⁴⁸ Eigen onderlijning van het Comité.

⁴⁹ Memorie van toelichting, pag. 61.

(10) VERSTORINGSOPDRACHT EN -BEVOEGDHEDEN

51. Momenteel hebben de VSSE en de ADIV (louter) de hoedanigheid van inlichtingen- en veiligheidsdienst. Het wetsontwerp stelt voor om beide diensten tevens de hoedanigheid te verlenen van actiedienst, niet enkel in het buitenland doch ook op Belgisch grondgebied. Dit houdt in dat beide diensten, naast de detectie en identificatie van nationale veiligheidsdreigingen en de doorgifte van de in dit kader bekomen onderzoeksresultaten aan andere overheden die deze informatie kunnen aanwenden in de uitoefening van hun bevoegdheden, door het wetsontwerp belast worden met het zelf nemen van offensieve maatregelen tegen dergelijke dreigingen. Het Comité merkt op dat dit een heuse paradigmashift is binnen de Belgische veiligheidsgemeenschap en roept daarom op dergelijke regeling niet zonder grondig democratisch debat in te voeren.

Omschrijving van de verstoringsoopdracht (ontwerp van art. 7, 5° en art. 11, §, 7° WIV)

52. De wijze waarop de nieuw toe te voegen verstoringsoopdracht *wettelijk omschreven* wordt in art. 7, 5° WIV (m.b.t. de VSSE) – “*het verstoren van de activiteiten bedoeld in artikel 7, 1° en 3°/1*” – en in art. 11, §1, 7° WIV (m.b.t. de ADIV) – “*de factoren, activiteiten of dreigingen bedoeld onder 1° tot en met 3° en 5° te verstoren*” – is op meerdere vlakken problematisch.

Zo is het Comité van oordeel dat de term “verstoren” veel te vaag is, zeker in het licht van de vereisten gesteld door artikel 22 Grondwet en artikel 8 EVRM. De wet geeft geen omschrijving van deze term zodat er op dit vlak weinig limieten zijn aan de mogelijkheden van de inlichtingendiensten. De voorgestelde regeling is ook (deels) onverenigbaar met de proportionaliteitsvereiste (bv. art. 8, tweede lid EVRM). De hier gebruikte bewoordingen gaan ook veel verder dan de bewoordingen in de memorie van toelichting en in het regeerakkoord 2025-2029.

Het Comité herinnert eraan dat art. 7, 1° handelt over “elke activiteit die (...) bedreigt of zou kunnen bedreigen”. Het gaat met andere woorden zowel over dreigingen (“elke activiteit die bedreigt”) alsook – en dit is problematisch in het licht van een verstoringsoopdracht – over potentiële dreigingen (“elke activiteit die zou kunnen bedreigen”). Een dergelijke omschrijving in art. 7, 1° is zonder meer gerechtvaardigd. Betrokken bepaling bevat immers de algemene inlichtingenopdracht. Het gaat hier over het inwinnen en analyseren van informatie met als oogmerk nagaan of er sprake is van een dreiging. In het licht van een verstoringsoopdracht zou een dergelijk woordgebruik evenwel tot gevolg hebben dat de VSSE wettelijk wordt toegelaten om verstoringssacties op te zetten tegen activiteiten die misschien een dreiging vormen, tegen activiteiten waarvan het m.a.w. niet vaststaat dat ze (reeds) een dreiging zijn. Niet enkel is dit disproportioneel, het mist ook elke vorm van doelmatigheid. De nationale veiligheid moet beschermd worden tegen dreigingen. Dit vereist dat de VSSE beschikt over concrete en afdoende informatie over een actuele dreiging. Verstoringssacties tegen activiteiten die nog niet als dreiging kunnen gekwalificeerd worden, zijn overigens willekeurig en horen volgens het Comité niet thuis in een democratische rechtstaat.

De omschrijving in art. 11, 7° is nog problematischer gezien in deze bepaling de dreigingsrelatie volledig wordt verlaten. Art. 11, §1, 1°, eerste onderdeel – dat de algemene inlichtingenopdracht van de ADIV bevat, meer bepaald de inlichtingensteun aan militaire operaties – stelt als voorwerp “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”. Net zoals bij art. 7, 1° wenst het Comité te benadrukken dat een dergelijk woordgebruik volledig gerechtvaardigd is in het kader van een inlichtingenopdracht. In het licht van een verstoringsoopdracht zou een dergelijk woordgebruik evenwel ten gevolge hebben dat de ADIV wettelijk wordt toegelaten om verstoringssacties op te zetten tegen activiteiten die elke link met enige dreiging missen.



Een dergelijke verwoording in het wetsontwerp is zoals hoger gezegd opmerkelijk gezien zowel de memorie van toelichting bij het wetsontwerp alsook de betrokken passage in het regeerakkoord 2025-2029 enkel spreken over “dreigingen” en nooit over “potentiële dreigingen”. Zo stelt het regeerakkoord 2025-2029: “Een weerbare overheid is in staat om dreigingen zoals spionage, inmenging, extremisme en terrorisme aan te pakken. Daar is een sterke inlichtingendienst voor nodig die niet alleen in staat is om deze dreigingen op tijd te detecteren, maar ook om ze tegen te gaan.”. En verder: “Via een herziening van de wet op de inlichtingen- en veiligheidsdiensten zorgen we ervoor dat de Veiligheid van de Staat, onder toezicht van de controleorganen, in staat gesteld wordt om dreigingen effectief tegen te gaan (disruptie).”.⁵⁰

Verder is het ook niet gerechtvaardigd dat punt 3° van art. 11, §1 in de wettelijke omschrijving van de verstoringsoopdracht wordt opgenomen. Betrokken bepaling bevat de opdracht inzake handhaving van de militaire veiligheid. Deze bestaat uit (1) de veiligheid van het personeel, de installaties, wapens en wapensystemen, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere voorwerpen van Defensie⁵¹, en (2) de veiligheidssteun aan militaire operaties⁵². Van belang in dit kader is o.m. het van de ADV afkomstige Reglement IF5 “Onderrichting van de Militaire Veiligheid” van 26 september 2023. Dit reglement omvat alle richtlijnen rond de militaire veiligheid binnen het ministerie van Landsverdediging. Betrokken bepaling bevat geen dreigingsoriëntatie, maar een beschermingsoriëntatie en heeft om die reden geen grondslag om opgenomen te worden in een verstoringsoopdracht gericht op het bestrijden van dreigingen.

Het Comité merkt voorts op dat verstoringssacties bijna per definitie (diep) ingrijpen in het privéleven van burgers (bv. iemand ostentatief volgen of zijn omgeving kenbaar maken dat hij een target is van een inlichtingendienst). Zij kunnen openlijk zijn naar de betrokkene, maar ook in het geheim plaatsvinden. Om potentieel misbruik te voorkomen, is het vaste rechtspraak van het Europees Mensenrechtenhof dat (*in casu* preventieve en geheime) maatregelen tegen dreigingen tegen de nationale veiligheid – willen ze verenigbaar zijn met het EVRM en in het bijzonder willen ze voldoen aan de vereisten gesteld aan de beperkingen op bepaalde mensenrechten (o.m. art. 8, tweede lid EVRM) – slechts toegelaten zijn ingeval er sprake is van een *ernstige en actuele* dreiging⁵³ van de nationale veiligheid.⁵⁴

Zowel het Europees Hof voor de Rechten van de Mens als het Grondwettelijk Hof oordelen dat een inmenging in het privéleven niet volstaat met een “formele” wettelijke basis. De wet moet ook voldoende toegankelijk, voorzienbaar en precies zijn. Art. 22 Grondwet vereist bovendien dat de wet zelf de essentiële toepassingsvoorwaarden en procedurele waarborgen bepaalt.

53. Vernoemde redenen noodzaken vooreerst een aanpassing van de omschrijving van de verstoringsoopdracht in volgende zin:

- art. 7: “het verstoren van de ernstige en actuele dreigingen zoals bedoeld in artikel 7, 1° en 3°/1”
- art. 11, §1: “het verstoren van de ernstige en actuele dreigingen zoals bedoeld onder 1° tot en met 2°/1° en 5°” (ADV-39).

Daarnaast moet een voldoende duidelijke definitie worden opgenomen van handelingen die onder deze bevoegdheid kunnen vallen.

⁵⁰ Regeerakkoord 2025-2029, pag. 142.

⁵¹ Art. 11, §1, 2°, eerste onderdeel WIV.

⁵² Art. 11, §1, 2°, eerste onderdeel WIV, vgl. art. 21, 1° KB Structuur Defensie (*a contrario*).

⁵³ Bv. arrest nr. 37138/14 d.d. 12 januari 2016 *Szabó en Vissy t. Hongarije* (2016), nr. 75;

⁵⁴ Om die reden wordt er bijvoorbeeld in art. 8bis Vreemdelingenwet vereist dat er sprake moet zijn van “een ernstige en daadwerkelijke bedreiging van de openbare orde of de nationale veiligheid” vooraleer bepaalde maatregelen genomen kunnen worden.



Zoals het Comité reeds heeft aanbevolen in zijn *Juridische analyse betreffende de wettelijke mogelijkheden waarover de inlichtingendiensten beschikken inzake verstoring* (nr. 2022.295 van 20 januari 2023), dient een verstoringsopdracht om juridisch-technische redenen te worden verankerd in de art. 7 WIV (m.n. opsomming VSSE-opdrachten) en art. 11 WIV (m.n. opsomming ADIV-opdrachten). Niettemin wenst het Comité eraan te herinneren dat een verstoringsactiviteit, gelet op artikel 22 van de Grondwet, slechts kan plaatsvinden wanneer zij strikt noodzakelijk is. Dergelijke activiteiten mogen geen routinematig karakter krijgen, maar dienen beperkt te blijven tot uitzonderlijke gevallen waarin de vereiste noodzaak afdoende is aangetoond.

54. Op legistiek vlak, in het bijzonder wat de plaats van de verstoringsopdracht (ADV-40) betreft, herinnert het Comité eraan dat sinds 2016 het punt 3° van art. 7 WIV een lege bepaling is gelet op de schrapping van de toenmalige protectieopdracht van de VSSE. Het is aangewezen om deze bepaling te gebruiken voor de nieuwe verstoringsopdracht van de VSSE, niet in het minst omdat punt 4° van art. 7 WIV een restbepaling is die ertoe noodzaakt dat deze op de laatste plaats staat in een wettelijke opsomming van opdrachten (art. 7, 4°: “het uitvoeren van alle andere opdrachten die haar door of krachtens de wet worden toevertrouwd”).

Eenzelfde opmerking geldt voor de positie van de verstoringsopdracht van de ADIV in art. 11, §1 WIV. Punt 6° van art. 11, §1 bevat eenzelfde restbepaling die ertoe noodzaakt dat deze op de laatste plaats staat in een wettelijke opsomming van opdrachten van de ADIV.

55. In het licht van bovenbeschreven opmerkingen behoeven eveneens het ontwerp van aanpassing van art. 9 WIV (m.n. de vorderingsbevoegdheid van de VSSE tegenover de ADIV) en het ontwerp van aanpassing van art. 11, §3 WIV (m.n. de vorderingsbevoegdheid van de ADIV tegenover de VSSE) aanpassing (ADV-41).

Het is overigens niet duidelijk waarom beide bepalingen legistiek op een verschillende manier worden gewijzigd.

Verstoringsprocedure (ontwerp van art. 19, tweede lid, ontwerp van art. 19/2 tot 19/6 WIV)

56. Het wetsontwerp en memorie van toelichting maken een onderscheid tussen twee vormen van verstoring. Enerzijds is er de verstoring onder de vorm van een inlichtingendoorgifte (cf. art. 19 WIV) waarbij de doorgifte desgevallend een strafbare inbreuk kan uitmaken (onderworpen aan actueel art. 13/1 WIV *dixit* de toelichting bij de wijzigingen van art. 19 WIV⁵⁵). In de memorie van toelichting wordt dit de “indirecte verstoring” genoemd.⁵⁶ Deze mogelijkheid om informatie en inlichtingen door te geven aan andere overheden die deze gegevens kunnen aanwenden in het kader van hun bevoegdheden, heeft altijd bestaan. Anderzijds is er de verstoring onder de vorm van een verstoringsactie (cf. ontwerp van art. 19/2 tot 19/6 WIV) waarbij de verstoringsactie desgevallend een strafbare inbreuk kan uitmaken (cf. ontwerp van art. 19/3 WIV). In de memorie van toelichting heet dit de “directe verstoring”.⁵⁷

57. Problematisch is dat het wetsontwerp, met uitzondering van de verstoringsactie die een strafbare inbreuk uitmaakt (en ook dit behoeft nuance; *infra*), de beslissing tot verstoring exclusief toekent aan het diensthoofd van de betrokken inlichtingendienst, die deze bevoegdheid zelfs kan delegeren. Niet enkel de bevoegdheid tot het uitvoeren van een goedgekeurde verstoringsactie wordt toegekend aan de inlichtingendiensten doch ook, en in de regel, de bevoegdheid om te beslissen tot de inzet ervan buiten elke voorafgaande onafhankelijke controle. Het Comité vestigt in dit kader de aandacht op een van zijn aanbevelingen aan de Kamercommissie belast met de opvolging van de in de parlementaire onderzoekscommissie Terroristische Aanslagen geformuleerde aanbevelingen:

⁵⁵ Memorie van toelichting, pag. 75.

⁵⁶ Eerder werd dit door de VSSE in haar interne regelgeving “secundaire verstoring” genoemd.

⁵⁷ Eerder werd dit door de VSSE in haar interne regelgeving “primaire verstoring” genoemd.

“Het Comité is [...] van oordeel dat in een democratische rechtstaat de primaire verstoringsactiviteiten van de VSSE (m.a.w. het eigenmachtig optreden van de inlichtingendienst tegen een activiteit die ze zelf als bedreiging heeft gekwalificeerd afzonderlijk gereguleerd moeten worden in een voldoende duidelijke wet in de formele zin van het woord. De achterliggende gedachte is dat er verschillende instanties verantwoordelijk moeten zijn voor het opsporen en onderzoeken van mogelijke nationale veiligheidsdreigingen, voor de dreigingsinschatting (in casu het beoordelen of personen, groeperingen of gebeurtenissen daadwerkelijk een nationale veiligheidsdreiging vormen) en voor het nemen van de nodige maatregelen tegen dergelijke dreigingen. Minstens dient de beslissingsmacht tot het executief optreden in handen te liggen van een instantie andere dan de uitvoerende instantie. Een alternatief bestaat in het inrichten van een externe controle vergelijkbaar met de BIM-controle.”⁵⁸

Een inlichtingendienst heeft de wettelijke mogelijkheid om een persoon of groepering zelf te ‘kwalificeren’ als een nationale veiligheidsdreiging. Het zijn echter de politieke, gerechtelijke, bestuurlijke, politionele of diplomatieke overheden die bestemming zijn van de informatie van de inlichtingendiensten die het laatste woord hebben en die over de bevoegdheid beschikken om al dan niet een tegenmaatregel te nemen binnen het kader van hun wettelijke opdrachten en bevoegdheden. Het wetsontwerp geeft laatstgenoemde bevoegdheid nu ook aan de VSSE en de ADIV. Het Comité merkt op dat diverse overheidsinstanties binnen de rechtshandhaving zowel bevoegdheden hebben om informatie in te winnen alsook om vervolgens tegenmaatregelen te nemen. Er zijn echter enkele fundamentele verschillen. Vooreerst is er in dergelijke gevallen een administratief of gerechtelijk dossier voorhanden met alle relevante informatie die in de regel toegankelijk is voor de betrokkene. Verder zijn de maatregelen die deze overheden kunnen nemen duidelijk omschreven in de wet en veruitwendigd via een gemotiveerde beslissing (hetgeen niet kan gezegd worden van de mogelijkheid om dreigingen te ‘verstoren’). En tot slot zijn dergelijke tegenmaatregelen aanvechtbaar voor en controleerbaar door een onafhankelijke rechterlijke instantie. Deze procedurele waarborgen ontbreken bij een verstoring door een inlichtingendienst zoals uitgewerkt in voorliggend ontwerp.

58. Het wetsontwerp voorziet enkel in de voorafgaande toestemming van de BIM-Commissie ingeval een verstoringssactie gepaard gaat met een strafbaar feit: ofwel onder de regeling in artikel 13/1 WIV ofwel onder de voorgestelde regeling in art. 19/3 WIV. Het onderscheidingscriterium, zijnde een verstoring die al dan niet een strafbaar feit uitmaakt, is volgens het Comité onvoldoende om tegemoet te komen aan een afdoende onafhankelijke externe controle op een verstoringssactie.

Daarenboven is er een ernstig risico dat een inlichtingendienst in een dossier beslist om een verstoringssactie te verrichten en om deze niet via de BIM-Commissie te laten passeren omdat de dienst verkeerdelijk van oordeel is dat er geen sprake is van een misdrijf. Anders gesteld: het gevaar is reëel dat een inlichtingendienst verkeerdelijk gebruik maakt van de procedure bedoeld in het ontwerp van art. 19/4 WIV daar waar gebruik moet worden gemaakt van de procedure bedoeld in het ontwerp van art. 19/3 WIV. De wetgever heeft net de BIM-Commissie, bestaande uit drie magistraten (onderzoeksrechter, (straf)rechter en parketmagistraat), in 2010 opgericht wegens de expertise van zijn leden in onderzoeksbevoegdheden en hun deskundigheid in strafzaken.

De memorie van toelichting zelf bevat voorbeelden van verstoringssacties die geen strafbaar feit zouden uitmaken: “agenten (die) een nepcamera zeer zichtbaar voor de woning van een persoon plaatsen wiens bedreigende activiteit de inlichtingendiensten willen verstoren” en “een opvallende schaduwingsoperaties (...) van een

⁵⁸ COMITÉ I, Toezichtonderzoek naar de opvolging van de in de parlementaire onderzoekscommissie Terroristische Aanslagen geformuleerde aanbevelingen met betrekking tot de inlichtingen- en veiligheidsdiensten, n° 2022.294 (www.comiteri.be) en COMITÉ I, Juridische analyse aangaande de wettelijke mogelijkheden waarover de inlichtingendiensten beschikken met betrekking tot verstoring, n° 2022.295 (www.comiteri.be).



persoon in het bijzijn van zijn contacten om hun relatie te verbranden”.⁵⁹ Beide acties kunnen onder de toepassing van het misdrijf belaging vallen (art. 442bis Sw-1867; art. 237 Sw-2024). Deze inbreuk omschrijft zich als “het opzettelijk ernstig verstoren van de rust van een persoon zelfs al is het eenmalig of bestaat het uit een enkele handeling terwijl men wist of had moeten weten dat men door dit gedrag de rust van die bewuste persoon ernstig zou verstoren”. Dit voorbeeld in de memorie van toelichting veruitwendigt op zich reeds de vereiste expertise binnen de strafrechtelijk kwalificatie.

Tot slot herinnert het Comité aan een passage in de memorie van toelichting bij de Wet van 14 juli 2022 tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (BS 5 augustus 2022). Meer bepaald wordt gesteld: “De woorden ‘de feiten die als strafbaar feit of strafbare feiten kunnen worden gekwalificeerd’ – bedoeld wordt de verplichte vermelding in de vraag van de inlichtingendienst aan de BIM-Commissie tot het plegen van misdrijven in het kader van een inlichtingenmethode (cf. art. 13/1, §3, vierde lid, 1° WIV) – “worden gebruikt opdat het verzoek de specifieke feiten die gepland zijn, omvat. Anderzijds wordt de kwalificatie zelf, die niet onder de bevoegdheid van een inlichtingendienst valt, overgelaten aan het oordeel van de Commissie.”.⁶⁰ Er bestaat geen objectieve rechtvaardiging waarom de BIM-Commissie bevoegd zou moeten zijn voor de strafrechtelijke kwalificatie van door de inlichtingendiensten voorgenomen activiteiten binnen het inwinnen van informatie die niet zou gelden bij het nemen van verstoringsacties. Meer zelfs, deze procedurele waarborg heeft nog meer belang bij laatstgenoemde activiteiten aangezien de impact ervan op individuen verder gaat. De beslissing dat bepaalde door de inlichtingendiensten voorgenomen activiteiten geen strafrechtelijke inbreuk met zich meebrengt, is overigens minstens even belangrijk en vereist minstens evenveel expertise als het vaststellen welke exacte strafrechtelijke inbreuk(en) een verstoringsactie met zich zou meebrengen. Dit gegeven op zich is volgens het Comité reeds afdoende om elke voorgenomen verstoringsactie voor te leggen aan de BIM-Commissie.

59. In het wetsontwerp beslist een inlichtingendienst aldus niet enkel zelf of ze een persoon of groepering als nationale veiligheidsdreiging beoordeelt, de dienst beslist ook zelf of er een verstoringsactie moet genomen worden tegen een dergelijke persoon of groepering, ze beslist zelf of een verstoringsactie tevens een strafrechtelijke inbreuk vormt en ze voert een verstoringsactie dan ook nog eens autonoom uit (zonder externe eerstelijnscontrole). Omwille van deze situatie adviseert het Comité negatief over het geheel van de in het wetsontwerp voorgestelde verstoringsprocedure, en dringt aan om de gehele verstoringsprocedure te herzien (ADV-42).

Het Comité herinnert aan het regeerakkoord 2025-2029 dat stelt dat “(...) onder toezicht van de controleorganen, (de Veiligheid van de Staat) in staat gesteld wordt om dreigingen effectief tegen te gaan (disruptie)”.⁶¹ De vereiste van een toezicht van de controleorganen is geenszins afdoende aanwezig in voorliggend wetsontwerp. Het Comité benadrukt dat een controle a posteriori – zoals de controle door het Comité overeenkomstig de Toezichtwet van 18 juli 1991 maar ook de maandelijkse notificatie aan het Comité voorzien in ontwerp art. 19/5, §7 WIV – dus nadat de verstoringsactie werd genomen, niet voldoet aan de vereiste van een voorafgaande, onafhankelijke en bindende controle. Stellen dat het Comité altijd een controle overeenkomstig de Toezichtwet kan uitvoeren komt derhalve niet tegemoet aan het wettelijk ontbreken van een a priori controle op alle verstoringsacties. Stellen zoals het ontwerp art. 19/5, §8 WIV dat “De Commissie en het Vast Comité I (...) te allen tijde een wettigheid van de in artikelen 19/3 en 19/4 bedoelde maatregelen (kunnen) controleren” is eveneens niet afdoende. Stellen dat de controleorganen “te allen tijde” een controle kunnen verrichten, verandert namelijk niets aan het feit dat er vooraf geen akkoord wordt gevraagd aan een onafhankelijk controleorgaan.

⁵⁹ Memorie van toelichting, pag. 78.

⁶⁰ Parl. St. Kamer 2021-2022, nr. 55-2706/001, 25.

⁶¹ Regeerakkoord 2025-2029, pag. 142.



60. Om aan boven beschreven problemen tegemoet te komen, dienen alle verstoringssacties voorafgaandelijk onderworpen te worden aan de toestemming van een externe autoriteit. De bestaande procedure bij de uitzonderlijke inlichtingenmethoden, waarbij elk geplande uitzonderlijke methode voorafgaandelijk onderworpen wordt aan de toestemming van de BIM-Commissie (het zgn. bindend/eensluidend advies) en waarbij in de tweede lijn een jurisdictioneel toezicht door het Comité wettelijk georganiseerd wordt, kan hierbij, desgevallend, als inspiratie dienst doen. Ze heeft haar nut en praktische en juridische weerbaarheid bewezen.

61. Een aanpassing dient ook te geschieden in het belang van de uitvoerende agenten van de inlichtingendiensten. Ingeval een inlichtingendienst beslist dat een verstoringssactie niet gepaard gaat met een misdrijf, terwijl dit later door de gerechtelijke autoriteiten anders wordt beoordeeld, betekent dit dat de uitvoerende agenten van de betrokken inlichtingendienst een misdrijf plegen zonder dat dit juridisch gedekt wordt. In dergelijk geval worden de uitvoerende agenten – doch ook het diensthoofd dat toestemming heeft gegeven – blootgesteld aan strafvervolgning, die desgevallend geïnitieerd kan worden door een burgerlijke partijstelling (bv. door het target dat voorwerp van de verstoring vormde).

62. Het Comité is voorts van oordeel dat de beslissing van het diensthoofd, zoals omschreven in het ontwerp van art. 19/3, §2 en bevattende diverse verplichte vermeldingen, van toepassing moet zijn op alle vormen van verstoring, ongeacht deze verstoring geschiedt via informatiedoorgifte (cf. ontwerp van tweede lid van art. 19 WIV) of via verstoringssactie, en ongeacht deze verstoring een strafbaar feit uitmaakt. Het verstoren is een te verregaande maatregel opdat de wetgever niet tussenbeide zou dienen te komen over de verplichte vormvereisten van een dergelijke beslissing.

Verstoring door de ADIV (de Krijgsmacht) op Belgisch grondgebied

63. Het Comité brengt in herinnering dat de ADIV een onderdeel is van de Krijgsmacht. Binnen de feitelijke uitvoering op het terrein is, in vredetijd, normaliter de politie belast met de inwendige veiligheid en is de Krijgsmacht bevoegd voor de uitwendige veiligheid. Onder bepaalde wettelijke en reglementaire voorwaarden kan de Krijgsmacht ook in vredetijd ingeschakeld worden op Belgisch grondgebied. De bevoegdheid van de ADIV om verstoringssacties te mogen uitvoeren op Belgisch grondgebied komt neer op het opereren van de Krijgsmacht op Belgisch grondgebied op een andere manier dan via louter inlichtingenwerk. Het Comité stelt vast dat in de memorie van toelichting aan dit aspect geen aandacht werd besteed. Het adviseert om dit voorwerp van debat te maken, en desgevallend een dergelijke activiteit te omkaderen met bijkomende vormen van politieke besluitvorming (ADV-43).

Verstoring door de ADIV in cyberspace

64. Door de verstoringsoopdracht toe te kennen aan de ADIV verkrijgt deze inlichtingendienst eveneens de bevoegdheid tot het verstoren in cyberspace. Krachtens het KB dat de algemene structuur van het ministerie van Landsverdediging bepaalt, bestaat binnen de ADIV een *Cybercommando* (Cyber Command) dat optreedt in het domein van cyberspace en dat de opdrachten uitvoert die bepaald zijn in artikel 11 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.⁶² Het Cybercommando moet (juridisch) onderscheiden worden van de *Cybermacht* (Cyber Force). Dit is een van de vijf machten (strijdkrachten) binnen de Belgische Krijgsmacht.⁶³

Het wetsontwerp zorgt ervoor dat de Cybercommando niet langer enkel bevoegdheden heeft binnen cyberintelligence en cybersecurity, doch ook de bevoegdheid verkrijgt om cyberaanvallen uit te voeren die

⁶² Cf. art. 42, eerste lid KB van 30 juni 2025 tot bepaling van de algemene structuur van het Ministerie van Landsverdediging en van de bevoegdheden van bepaalde autoriteiten (BS 15 juli 2025; hierna: KB Structuur Defensie).

⁶³ Naast de Landmacht, Luchtmacht, Marine en Medische dienst (cf. art. 1, eerste lid, 5° KB Structuur Defensie).



niet louter een tegenaanval betreffen doch ook om verstoringssacties in cyberspace uit te voeren. In het licht hiervan en indachtig het onderscheid tussen Cybercommando en Cybermacht stelt zich de vraag welke offensieve cyberactiviteiten wettelijk nog zouden kunnen toegewezen worden aan de Cybermacht, andere dan degene die vallen onder het toepassingsgebied van de verstoringssacties zoals bedoeld in het ontwerp van art. 19/2 tot 19/6 WIV. Het Comité adviseert om dit nader te bepalen in de memorie van toelichting (ADV-44).

Aanvullend adviseert het Comité om in de wet een definitie te geven van het begrip “cyberaanval” (ADV-45), alsook of en in welke mate dit begrip samenvalt met een verstoringssactie in cyberspace.

Verboden verstoringssacties

65. Het wetsontwerp bevat een verbod op geweld (ontwerp van art. 19/2, tweede lid WIV) en een verbod op aantasting van een strafonderzoek (ontwerp van aanpassing van art. 13/5 WIV) tijdens een verstoringssactie. Het Comité onderschrijft het belang van beide verbodsbepalingen.

Wel wenst het Comité op te merken dat de omschrijving van het verbod op geweld een aanvulling behoeft. Momenteel staat er: *“De verstoring mag in geen geval opzettelijk afbreuk doen aan de fysieke integriteit van personen.”* Het Comité merkt op dat enkel de *“opzettelijke”* aantastingen van de fysieke integriteit expliciet worden verboden. Aantastingen van de fysieke integriteit wegens een, al dan niet ernstig *“gebrek aan voorzorg en voorzichtigheid”* vallen niet onder de toepassing van deze verbodsbepaling. Een verstoringssactie die aldus schade veroorzaakt aan iemands fysieke integriteit wegens een (ernstige) onvoorzichtigheid of een (ernstig) gebrek aan voorzorg in hoofde van de VSSE of de ADIV of in hoofde van een derde die handelt in opdracht van een inlichtingendienst maakt geen voorwerp van betrokken bepaling. Zo laat het ontwerp in zijn huidige vorm bijvoorbeeld toe dat de VSSE/ADIV binnen een groepering het (valse) gerucht zou verspreiden dat persoon X informant is. Los van het feit dat het Comité van oordeel is dat dergelijke ‘acties’ ver buiten de grenzen van het toelaatbare liggen, kan dit aanleiding geven tot represailles door derden. Een ruimer omschreven verbod zal de diensten er attent op maken dat elke verstoringssactie een gedegen voorbereiding en uitvoering eist. In dergelijk geval dreigt de federale Staat burgerlijk aansprakelijk gesteld te worden wegens een handeling van een inlichtingendienst. Het Comité vraagt om, in het ontwerp art. 19/2 en art. 19/6 §1, ofwel de woorden “door een gebrek aan voorzorg en voorzichtigheid” toe te voegen ofwel om het woord “opzettelijk” te schrappen (ADV-46).

66. Voorts wordt in het wetsontwerp het woord “opzettelijk” eveneens gevoegd in de art. 13/1, §4, art. 13/1/1, §3 en art. 18/10, §3/1, laatste lid. Het Comité is van oordeel dat ook deze bepalingen eenzelfde aanpassing behoeven (ADV-47).

67. Het Comité is van oordeel dat het verbod op geweld ook expliciet van toepassing moet gesteld worden op het verstoren via informatiedoorgifte gegrond op ontwerp art. 19, tweede lid WIV (communicatie aan het target zelf of aan derden die de verstoring kunnen uitvoeren) en op het aangepaste art. 19, derde lid (communicatie aan pers en publiek) (ADV-48). Een wettelijk voorschrift in de zin van *“De verstoring mag in geen geval opzettelijk of door een gebrek een voorzorg of voorzichtigheid afbreuk doen aan de fysieke integriteit van personen.”* moet de VSSE en de ADIV er attent op maken en verantwoordelijk voor stellen dat gevoelige informatie doorgeven aan bepaalde derden of zelfs aan het ruime publiek niet altijd onschuldig is en personen kan aanzetten tot het plegen van geweldsdaden. Het Comité is het er niet mee eens dat de inlichtingendiensten nooit verantwoordelijk kunnen zijn voor de handelingen die door derden gesteld worden gebruik makende van de informatie van de inlichtingendiensten, zeker wanneer dergelijke informatie door de inlichtingendiensten publiek wordt gemaakt vanuit een verstoringssfinaliteit.

68. Daarnaast is het Comité van oordeel dat beide verbodsbepalingen niet afdoende zijn. Het Comité erkent dat bepaalde maatschappelijke evoluties noodzaken tot meer bevoegdheden voor de VSSE en de ADIV. Tegelijkertijd dient dit te gebeuren met bepaalde grenzen die door de wetgever dienen aangebracht te worden. Om die reden moet er volgens het Comité eveneens een expliciet wettelijk verbod worden voorzien om onder de noemer van verstoringsacties politieactiviteiten uit te oefenen (ADV-49).

Uit het regeerakkoord, noch uit de memorie van toelichting blijkt enige wil om de VSSE en de ADIV om te vormen tot een politiedienst. Echter, wegens het ontbreken van een inhoudelijke omschrijving van een verstoringssactie – buiten enkele casuïstische voorbeelden in de memorie van toelichting en buiten een verwijzing naar het woordenboek (Van Dale en Le Robert) – is er geen enkele wettelijke garantie dat voor de toekomst hierboven beschreven verstoringssacties worden uitgesloten.

69. De Grondwet en internationale verdragen garanderen het genot van een aantal fundamentele rechten. Voor sommige daarvan is een beperking door de Staat mogelijk, mits een wettelijke tussenkomst en de naleving van de criteria van noodzakelijkheid en proportionaliteit. Voor andere is geen enkele afwijking toegestaan (bijv. het verbod op foltering en onmenselijke of vernederende behandelingen). Dit aspect wordt in het wetsontwerp niet behandeld, hoewel een verstoringssactie, zonder dat deze noodzakelijkerwijs een misdrijf vormt, tot gevolg kan hebben dat deze fundamentele rechten worden aangetast. Bij wijze van voorbeeld kan men zich, wat betreft het recht op leven of het verbod op onmenselijke en vernederende behandelingen, het geval voorstellen van een mededeling van persoonsgegevens van een individu dat een bedreiging vormt, indien deze informatie wordt meegedeeld aan een partnerdienst die acties zou ondernemen ten aanzien van die persoon.

Het Comité is van oordeel dat dergelijke scenario's, die in het huidige ontwerp mogelijk en niet verboden zijn, het voorwerp moeten uitmaken van een specifiek wettelijk kader, door te voorzien in een gesloten lijst van verboden (of andersom: toegelaten) verstoringshandelingen en een passende machtigings- en controleregeling voor verstoringen die een negatieve impact hebben op een fundamenteel recht dat door de Grondwet of een internationaal verdrag wordt gegarandeerd (ADV-50). Bij wijze van voorbeeld voorziet het Canadese recht in een machtigingsprocedure door een onafhankelijke autoriteit voor verstoringen die de fundamentele rechten van een individu zouden kunnen schaden of die in strijd zijn met het Canadese recht.⁶⁴

Verstoring tegen politieke mandatarissen

70. In zijn Activiteitenverslag 2021 schreef het Comité: “Veelvuldig werd in (parlementaire) debatten de vraag gesteld of en in welke mate de Belgische inlichtingendiensten politieke mandatarissen (mogen) opvolgen en welke regels ze daarbij in acht moeten nemen. Vanaf begin 2018 wordt in deze binnen de VSSE een als ‘vertrouwelijk’ geclassificeerde dienstnota toegepast. Conform deze nota, die werd geactualiseerd in juni 2020⁶⁵, zendt de VSSE twee types van rapporten naar de minister van Justitie en de Premier, met kopie naar het Vast Comité I. Het betreft enerzijds punctuele rapporten over politieke mandatarissen die bijdragen aan de totstandkoming van een dreiging alsook een trimestrieel overzicht van het geheel van documenten waarin melding wordt gemaakt van deze mandatarissen. De minister van Justitie stemde daarbij in met het ‘principe de vérifications par le Comité R qui s’avèrent nécessaires conformément à la loi organique du 18 juillet 1991’.⁶⁶ Gezien nergens wordt vermeld wat het Comité wordt geacht aan te vangen met voormelde informatie, nam het zelf het initiatief een methodo-

⁶⁴ Section 12.1 van de Canadian Security Intelligence Service Act (R.S.C., 1985, c. C-23).

⁶⁵ Deze geactualiseerde dienstnota is, in tegenstelling tot eerdere dienstnota, niet geclassificeerd.

⁶⁶ In: Brief van de minister van Justitie gericht aan het Comité I d.d. 26 juli 2018 over ‘Le recueil d’informations par un service de renseignement concernant une personne exerçant un mandat politique’, vermeld in: COMITÉ I, Activiteitenverslag 2021, pag. 32, voetnoot 59.

logie uit te werken omtrent de 'problematiek van de opvolging van de politieke mandatarissen door de inlichtingendiensten en de rol van het Vast Comité I'. Deze methodologie werd in 2020 door de parlementaire Begeleidingscommissie goedgekeurd."⁶⁷

De bedoelde politieke mandatarissen zijn de ministers van de diverse regeringen, de Belgische commissaris in de Europese Commissie en de leden van de verschillende Parlementen, inclusief de Belgische leden van het Europees Parlement. Het gaat niet om andere verkozenen of aangeduide mandatarissen (bijv. op gemeentelijk vlak, zoals schepenen, of op provinciaal vlak, bijv. de gouverneurs).⁶⁸

Verder wordt gesteld: *"Politieke mandatarissen worden in de operationele werking van de VSSE niet anders behandeld dan andere beroepsgroepen. Indien er redenen zijn om de eventuele betrokkenheid van een politieke mandataris bij de totstandkoming van een dreiging nader te bekijken, dan dient dit ook te gebeuren. Behalve natuurlijk in die gevallen waarbij de politieke mandataris als slachtoffer betrokken is bij de totstandkoming van een dreiging. Omdat het om politieke mandatarissen gaat dienen wel een aantal mechanismen toegepast te worden opdat de dienst geen misbruik zou maken van haar positie. Met name de plicht om bevoegde ministers te informeren van zodra er een vermoeden ontstaat dat een politieke mandataris bijdraagt tot de totstandkoming van een dreiging, is één van die mechanismen."*⁶⁹

In zijn Juridische analyse aangaande de wettelijke mogelijkheden waarover de inlichtingendiensten beschikken met betrekking tot verstoring – ook vermeld in de memorie van toelichting – stelt het Comité: *"Uit de dienstnota's n° 20-28 en n° 20-29 blijkt duidelijk dat de VSSE zichzelf bevoegd acht om verstorend op te treden tegen als problematisch gekwalificeerde activiteiten van federale en regionale parlementsleden en ministers, en dit klaarblijkelijk niet enkel voor secundaire disruptie (m.n. het inkennisstellen en adviseren van de bevoegde instanties) maar ook voor primaire disruptie (m.n. zelf executief optreden)."*⁷⁰

In het voorliggend wetsontwerp wordt geen aandacht besteed aan het nemen van verstoringssacties tegenover politieke mandatarissen die, volgens de beoordeling van de betrokken inlichtingendienst, een nationale veiligheidsdreiging vormen. Het Comité adviseert om dit het voorwerp van debat te maken en, desgevallend, om bijkomende procedurele voorwaarden hieromtrent in de wet te voorzien (ADV-51).

Verstoring via informatiedoorgifte versus verstoring via verstoringssactie

71. Met betrekking tot een verstoring via informatiedoorgifte (ontwerp van art. 19, tweede lid WIV) geeft de memorie van toelichting o.m. volgend voorbeeld:

*"Deze boodschap kan expliciet zijn, zoals het briefje in de brievenbus, of impliciet. Communicatie moet in de brede zin worden opgevat: ze kan schriftelijk, mondeling of non-verbaal zijn. Non-verbale communicatie van informatie aan de persoon die door de inlichtingendiensten wordt gevolgd met het oog op een verstoring, kan dus indirect het resultaat zijn van een methode van informatiegaring, bijvoorbeeld tijdens een clandestiene inspectie in de woning van de persoon om het materiaal dat hij in zijn bezit heeft te inventariseren. De inlichtingenagenten laten dan opzettelijk sporen achter van hun bezoek, waarmee ze de boodschap "we weten wat u van plan bent" overbrengen."*⁷¹

⁶⁷ COMITÉ I, Activiteitenverslag 2021, 32-33.

⁶⁸ Dienstnota n° 20-28, pag. 2, vermeld in: COMITÉ I, Juridische analyse aangaande de wettelijke mogelijkheden waarover de inlichtingendiensten beschikken met betrekking tot verstoring, toezichtonderzoek nr. 2022.295, d.d. 20 januari 2023, pag. 2..

⁶⁹ Dienstnota van de VSSE n° 20-28, pag. 4-5, vermeld in: COMITÉ I, toezichtonderzoek nr. 2022.295, pag. 21.

⁷⁰ COMITÉ I, toezichtonderzoek nr. 2022.295, pag. 21.

⁷¹ Memorie van toelichting, pag. 73.



Het Comité is van oordeel dat dergelijke “non-verbale communicatie”⁷² niet onder de toepassing van ontwerp art. 19, tweede lid WIV valt (m.n. informatiedoorgifte) maar onder de toepassing van het ontwerp van art. 19/2 tot 19/6 WIV (m.n. verstoringssactie). Het gaat hier geenszins om de doorgifte en verstrekking van informatie aan derde (overheids)instantie waarop deze derde de mogelijkheid heeft om op basis van deze informatie maatregelen tegen betrokkene te nemen, maar om het zelf nemen van tegenmaatregelen. Het betreft m.a.w. het zelf executief optreden met als onmiddellijk opzet het verstoren van een dreiging.

Voorts illustreert het voorbeeld dat niet enkel het onderscheidscriterium ‘plegen van misdrijven’ binnen het nemen van verstoringssacties (ontwerp art. 19/2 tot 19/6 WIV) onwerkzaam is, maar dat ook het onderscheid tussen verstoring via informatiedoorgifte (ontwerp art. 19, tweede lid WIV) en verstoring via verstoringssactie vaak onduidelijk is en in de praktijk onwerkzaam zal zijn.

72. Het ontwerp van art. 19/5, §9 stelt: *“De artikelen 19/3 en 19/4 zijn niet van toepassing op de verstoring verricht in uitvoering van artikel 19 of in de uitoefening van andere opdrachten die aan de inlichtingen- en veiligheidsdiensten worden toevertrouwd door of krachtens de wet.”*. In de memorie van toelichting wordt zo’n ander voorbeeld gegeven: *“(h)et uitvoeren van veiligheidsonderzoeken in het kader van de afgifte van veiligheidsmachtigingen zoals beschreven in artikel 7, 2°, en 11, 4°”*⁷³ alsook andere soorten veiligheidsscreenings (bv. veiligheidsverificaties).⁷⁴

Wegens boven beschreven redenen is het Comité van oordeel dat een verstoring via informatiedoorgifte (cf. het ontwerp art. 19, tweede lid WIV), een verstoring via verstoringssactie die geen strafbare inbreuk uitmaakt en een verstoring via verstoringssactie die wel een strafbare inbreuk uitmaakt aan eenzelfde procedure, met eenzelfde materiële en formele voorwaarden moet onderworpen worden.

73. Tot slot stelt de memorie van toelichting dat *“Dergelijke verstoringen”* – bedoeld worden degene via informatiedoorgifte cf. art. 19 WIV (nvda) – *“zullen slechts worden ondernomen na een grondige risicoanalyse die het proportionele karakter van de verstoring aantoont: een evenwicht tussen het nagestreefde doel om een bedreigende activiteit tegen te gaan gelet op haar ernst en de gevolgen daarvan.”*. Het Comité juicht de vereiste van een risicoanalyse toe. Het is wel van oordeel dat het opstellen ervan in de wet verplicht moet worden, en dat de memorie van toelichting de verschillende aspecten dient te vermelden en omschrijven die in een dergelijke risicoanalyse minstens aan bod dienen te komen, waaronder de aard van de te controleren risico's (bv. operationele risico's, juridische risico's, veiligheidsrisico's, ...). De risicoanalyse moet geformaliseerd worden en deel uitmaken van het dossier dat ter beschikking wordt gesteld van de controlerende instantie(s) (ADV-52).

Subsidiariteit en proportionaliteit

74. Elke verstoringssactie moet logischerwijs voldoen aan de proportionaliteitsvereiste én de subsidiariteitsvereiste. Het ontwerp van art. 19/3, §2, 6° WIV bevestigt dit door te eisen dat *“de subsidiariteit en proportionaliteit zoals bedoeld in artikel 19/5”* moeten omschreven worden in de beslissing van het diensthoofd. Het ontwerp van art. 19/5, §1 stelt: *“De in artikelen 19/3 en 19/4 bedoelde beslissing van het diensthoofd wordt afdoende gemotiveerd wat betreft de proportionaliteit en subsidiariteit van de verstoring”*. Laatstgenoemde bepaling verwoordt duidelijk dat beide beginselen bijgevolg moeten nageleefd worden bij elke verstoringssactie, ongeacht of deze al dan niet een strafbare inbreuk uitmaakt.

⁷² Ibid.

⁷³ Memorie van toelichting, pag. 7.

⁷⁴ Memorie van toelichting, pag. 79.

Het Comité vestigt de aandacht op het feit dat het ontwerp van art. 19/2 enkel een wettelijke definitie bevat van de proportionaliteitsvereiste. Het Comité is van oordeel dat ook de subsidiariteitsvereiste in betrokken bepaling wettelijk omschreven moet worden (ADV-53).⁷⁵ Hierbij moet volgens het Comité subsidiariteit zowel betrekking hebben op de *noodzakelijkheid voor de bestrijding van de betrokken nationale veiligheidsdreiging* alsook op het feit dat *maatregelen andere dan een verstoringssactie ontoereikend lijken te zijn*. Hierbij wijst het gebruik van de woorden “lijken te zijn” erop dat andere maatregelen niet daadwerkelijk eerst moeten geprobeerd worden, doch wel dat dit uit de motivering en het ontwerp van beslissing geacht wordt zo te zijn.

Concrete informatie

75. Nergens in het wetsontwerp wordt vereist dat de VSSE en de ADIV slechts dreigingen kunnen verstoren wanneer ze over concrete informatie beschikken over het bestaan van een dergelijke dreiging. Het Comité is van oordeel dat geruchten of vage vermoedens niet volstaat van dergelijke verregaande maatregelen. Zeker wanneer maatregelen worden genomen met negatieve gevolgen voor fysieke of rechtspersonen vereisen de algemene beginselen van behoorlijk bestuur dat een overheid afdoende concrete informatie beschikt om een maatregel te dragen. Desgevallend stellen dat de VSSE en de ADIV inlichtingendiensten zijn die geen bewijzen verzamelen doch louter inlichtingen mist elke grondslag als deze informatie gebruikt wordt om maatregelen op te laten steunen. Het Comité vraagt om dit te bevestigen in de memorie van toelichting (ADV-54).

Regulariseringsprocedure

76. Ontwerp art. 19/5, §5 WIV stelt: *“Indien, in het kader van een in de artikelen 7, 5° en 11, 7° bedoelde verstoring, door onvoorziene omstandigheden feiten worden gepleegd die een strafbaar feit of strafbare feiten kunnen uitmaken en waarvoor de in artikel 19/3 bedoelde procedure niet kon worden gevolgd, stelt het diensthoofd de Commissie hiervan zo spoedig mogelijk en uiterlijk op de eerstvolgende werkdag nadat hij kennis heeft genomen van het plegen van de feiten die een strafbaar feit of strafbare feiten kunnen uitmaken, schriftelijk in kennis. Indien de Commissie oordeelt dat de feiten in het kader van de in de artikelen 7, 5° en 11, 7° bedoelde verstoring werden gepleegd, maken zij geen strafbare feiten uit.”*

77. Het Comité stelt vast dat in de bestaande procedure in artt. 13/1 en 13/1/1 WIV – m.n. het plegen van misdrijven in het kader van de informatiegaring – geopteerd wordt voor het instrument van de strafuitsluitende verschoningsgrond en in de voorgestelde procedure in art. 19/2 ev. WIV – m.n. het plegen van misdrijven in het kader van een verstoringssactie – voor een rechtvaardigingsgrond. Het Comité vraagt om ofwel in beide gevallen een strafuitsluitende verschoningsgrond te hanteren, ofwel om in de memorie van toelichting het onderscheid nader te rechtvaardigen (ADV-55).

Voorts stelt het Comité vast dat in de memorie van toelichting lijkt gesteld te worden dat ook in het kader van een verstoring conform ontwerp art. 19, tweede lid – m.n. verstoring via communicatie o.m. aan een target – misdrijven kunnen worden gepleegd. Het Comité vraagt om dit aspect te verduidelijken (ADV-56). Aan gezien art. 19 WIV geen eigen procedure bevat voor het plegen van misdrijven zou in dergelijk geval gebruik moeten worden gemaakt van de procedure in art. 13/1 of 13/1/1 WIV (waar aldus de wetgever opteerde voor een strafuitsluitende verschoningsgrond). Ingeval dit een correcte lezing is, vraagt het Comité ofwel om, net zoals bovenstaande, eenzelfde strafrechtelijk instrument te hanteren, ofwel om in de memorie van toelichting dit onderscheid te rechtvaardigen.

⁷⁵ Ook bij de toepassing van specifieke en uitzonderlijke methoden bevat de Inlichtingenwet zowel een wettelijke definitie van de proportionaliteitsvereiste alsook van de subsidiariteitsvereiste.



78. Het Comité brengt onder de aandacht dat voorliggende regularisatieprocedure – die gebaseerd is op de regularisatieprocedure beschreven in art. 13/1, §7 WIV – louter van toepassing kan zijn bij onvoorziene omstandigheden. Deze procedure kan bijgevolg niet van toepassing zijn ingeval een inlichtingendienst een verstoringsactie heeft gepleegd onder art. 19/4 WIV (enkel beslissing diensthoofd, geen vereiste van voorafgaand akkoord BIM-Commissie) daar waar nadien blijkt dat dit onder art. 19/3 WIV had moeten zijn (met vereiste van voorafgaand akkoord BIM-Commissie). In dergelijk geval gaat het immers niet om onvoorziene omstandigheden. De activiteiten die de verstoringsactie omvatten zullen immers voordien zijn gekend, en zijn bijgevolg altijd voorzienbaar. Ook om deze reden pleit het Comité om een uniforme procedure in te richten ongeacht een verstoringsactie al dan niet een strafrechtelijke inbreuk uitmaakt.

79. Het Comité stelt vast dat in de bestaande regularisatieprocedure in art. 13/1, §7 WIV de BIM-Commissie ook de onvoorzienbaarheid moet controleren: *“De agent die deze feiten heeft gepleegd blijft vrij van straf indien de Commissie oordeelt dat zij niet voorzienbaar en strikt noodzakelijk waren ter verzekering van de eigen veiligheid of die van derden.”*. In de voorgestelde regularisatieprocedure in ontwerp art. 19/5, §5 is dit niet bepaald: *“Indien de Commissie oordeelt dat de feiten in het kader van de in de artikelen 7, 5° en 11, 7° bedoelde verstoring werden gepleegd, maken zij geen strafbare feiten uit.”*. Het Comité is van oordeel dat een controle door de BIM-Commissie op de onvoorzienbaarheid van de strafbare feiten fundamenteel is. In het kader van een verstoringsactie is dit nog meer het geval gezien de beslissing van de BIM-Commissie de wederrechtelijkheid van de strafbare feiten wegneemt, daar waar in het kader van art. 13/1, §7 de wederrechtelijkheid blijft maar, in beginsel, geen strafrechtelijke sanctie kan worden gevorderd of opgelegd. Het Comité is van oordeel dat ook binnen de regularisatieprocedure bij verstoringsacties de BIM-Commissie de onvoorzienbaarheid dient te controleren. Het is van oordeel dat dit dient toegevoegd te worden in de wet (ADV-57).

Samenloop strafonderzoek

80. Uit ontwerp art. 19/3, §2, tweede lid WIV blijkt dat de vermelding van “de samenloop” – van een verstoringsactie – “met een opsporings- of gerechtelijk onderzoek” (§2, eerste lid, 7°) als vermelding in de beslissing van het diensthoofd van de inlichtingendienst niet voorgeschreven is op straffe van onwettigheid. Het Comité herinnert eraan dat een nationale veiligheidsdreiging veelal tevens een inbreuk op de strafwet zal betekenen, zeker voor wat betreft de dreigingen die tot de bevoegdheid van de VSSE behoren (zie bijvoorbeeld: de recente actualisering van het spionagemisdrijf, de recente strafbaarstelling van het inmengingsmisdrijf, de ruime draagwijdte van het terrorismemisdrijf). Vanuit deze invalshoek is het Comité van oordeel dat betrokken vermelding wel op straffe van onwettigheid moet voorgeschreven zijn (ADV-58).

Toezicht door de BIM-Commissie en het Comité I

81. Naast de elders uiteengezette problemen kampt het ontworpen artikel 19/5, §8, dat voorziet in een wettelijkheidscontrole door de BIM-commissie en het Comité op de in de ontworpen artikelen 19/3 en 19/4 bedoelde verstoringen, met een gebrek aan precisie over de wijze waarop deze twee organen hun toezicht dienen uit te oefenen. In het kader van het toezicht op de bijzondere inlichtingenmethoden is de volgorde waarin de twee organen optreden beschreven, en deze komt in grote lijnen overeen met een voorafgaand en realtime toezicht respectievelijk een controle a posteriori. Hierbij is het toezicht van de BIM-Commissie een administratieve eerstelijnscontrole en is het toezicht van het Comité I een tweedelijnscontrole die jurisdictioneel van aard is. Evenzo is in het kader van bepaalde beschermings- en ondersteuningsmaatregelen (bv. het plegen van misdrijven) bepaald dat de BIM-commissie een beslissing neemt, waartegen de inlichtingendienst desgevallend beroep kan aantekenen bij het Comité.

In voorliggende regeling is er in geen enkel mechanisme voorzien, wat het risico inhoudt dat er een concurrerende bevoegdheid tussen de twee instellingen ontstaat. Het Comité beveelt daarom aan om, in het kader van de bepleite ruimere herziening van deze materie, de respectievelijke toezichtsmodaliteiten van de



BIM-commissie en het Comité nauwkeurig vast te leggen, en te bepalen hoe deze vormen van toezicht op elkaar aansluiten (ADV-59).

Taalkundige opmerkingen in ontwerp van art. 19, tweede lid WIV

82. Ontwerp art. 19, tweede lid WIV: *“De inlichtingen- en veiligheidsdiensten kunnen informatie en persoonsgegevens meedelen aan personen of instanties die het onderwerp uitmaken van een verstoring bedoeld in de artikelen 7, 5° en 11, 7°, of die bijdragen tot de uitvoering van deze verstoring.”.*

Het Comité stelt voor om (ADV-60):

- in de Nederlandstalige versie het begrip “onderwerp” te vervangen door het begrip “voorwerp”
- het begrip “informatie” – die binnen de inlichtingengemeenschap verwijst naar de brute gegevens – wordt vervangen door het begrip “inlichtingen” – die verwijst naar verwerkte informatie.

83. Zowel ontwerp art. 19/3, §1, eerste lid als ontwerp art. 19/4, §1, eerste lid stellen in de Franstalige versie op eenzelfde wijze: *“Sous réserve de l'article 19 et d'autres dispositions spécifiques aux missions (...)”.* Het Comité stelt vast dat in beide artikelen deze zin anders wordt vertaald. Om verwarring te vermijden adviseert het Comité om ook in de Nederlandstalige versie een exacte vertaling te voorzien (ADV-61).

84. Zowel ontwerp art. 19/3, §1, tweede lid als ontwerp art. 19/4, §1, tweede lid bevatten het begrip “GAS-inbreuken” (ADV-62). Voor de aanpassing hiervan verwijst het Comité voor de bespreking van de voorgestelde aanpassingen in art. 13/1 WIV.

(11) VORDERING MEDEWERKING VAN DERDEN (ontwerp art. 18/10, § 3/1-§3/4 en art. 19/6 WIV)

85. Het wetsontwerp creëert een strafrechtelijk gesanctioneerde vorderingsbevoegdheid tot medewerking van derden bij de aanwending van uitzonderlijke inlichtingenmethoden (ontwerp art. 18/10, §3/1 - §3/4 WIV) en bij de uitvoering van verstoringsoopdrachten (ontwerp art. 19/6, §1 - §6 WIV).

Op grond van beide bepalingen kan *iedereen*, in vredetijd, in het binnen- en buitenland, ongeacht zijn hoedanigheid (bv. politieambtenaren, leden openbaar bestuur), ongeacht een eventueel beschermd statuut (bv. minderjarigen, advocaten, journalisten, artsen), onder strafsancie verplicht worden om mee te werken met de VSSE en de ADIV. Beide regelingen ontbreken ook een daadwerkelijke inhoudelijke omschrijving, laat staan beperking, wat deze medewerking exact kan betekenen.

Vorderingsbevoegdheid bij de aanwending van uitzonderlijke methoden

86. Wat betreft deze vorderingsbevoegdheid is het voor het Comité onduidelijk welk soort vormen van medewerking onder het toepassingsgebied vallen. Art. 18/10, §3/1 spreekt van een “medewerking overeenkomstig artikel 13/4”. Laatstgenoemde bepaling geeft evenwel geen nadere omschrijving hiervan. De memorie van toelichting stelt dat het gaat over *“externe deskundigen of actoren die beschikken over specifieke technische bekwaamheid, infrastructuur of toegangsmogelijkheden die essentieel zijn voor de doeltreffende uitvoering van de opdracht”*.⁷⁶ Daarnaast worden er nog een aantal voorbeelden hiervan opgesomd.⁷⁷ Deze toelichting is voor het Comité ruim onvoldoende, te meer het wetsontwerp een weigering tot medewerking strafrechtelijk sanc-tioneert. Zo stelt zich onder meer de vraag of bijvoorbeeld elke persoon strafrechtelijk verplicht kan worden

⁷⁶ Memorie van toelichting, pag. 13.

⁷⁷ Memorie van toelichting, pag. 64.

om zijn woning ter beschikking te stellen aan de VSSE of de ADIV in het kader van een observatieopdracht (art. 18/11 WIV). Ook stelt zich de vraag of bijvoorbeeld een slotenmaker op basis van betrokken bepaling zich blootstelt aan strafrechtelijke vervolging wanneer hij weigert om een inlichtingendienst te helpen bij de doorzoeking van een woning of private plaats (art. 18/12 WIV), of als een boekhouder of een advocaat strafbaar zijn wanneer ze weigeren mee te helpen aan het opzetten door de VSSE of de ADIV van een bedrijf (frontstore) die als doel heeft om informatie te verzamelen (art. 18/13 WIV). De in het wetsontwerp uitgewerkte regeling is té algemeen en té verregaand. Het Comité adviseert negatief en vraagt met klem om de gehele regeling ofwel geheel te herzien rekening houdende met vernoemde opmerkingen ofwel te schrappen (ADV-63).

Voorts stelt zich de vraag hoe deze nieuwe vorderingsbevoegdheid bij de aanwending van uitzonderlijke methoden zich verhoudt ten opzichte van de reeds bestaande vorderingsbevoegdheden bij uitzonderlijke methoden? In het bijzonder gaat het dan over de vorderingsbevoegdheid tegenover postoperators (art. 18/14 WIV), operators van elektronische communicatienetwerken en verstrekkers van elektronische communicatiediensten (art. 18/17 WIV), bepaalde financiële instellingen (art. 18/15 WIV), en bepaalde deskundigen in informaticasystemen en -diensten (art. 18/16 WIV).

87. In art. 18/10, §3/1 wordt gesteld dat deze medewerking gevorderd kan worden *“in geval van ofwel een ernstig gevaar voor de fysieke integriteit van één of meer personen, ofwel van activiteiten verband houdend met terrorisme of met criminele organisaties”*. Het Comité brengt vooreerst in herinnering dat de begrippen “terrorisme” en “criminele organisatie” in de Inlichtingenwet een eigen invulling hebben die, deels ruimer, deels enger is dan deze begrippen binnen het Strafwetboek. Het Comité vraagt te verduidelijken over welke betekenis het gaat (ADV-64). Daarenboven betreffen het kwalificaties die in een inlichtingencontext relatief snel ingeroepen kunnen worden.

Vorderingsbevoegdheid bij de uitvoering van verstoringsopdrachten

88. Wat betreft deze vorderingsbevoegdheid stelt de memorie van toelichting *“dat de reikwijdte van de medewerkingsplicht in het kader van verstoring ruimer is”*.⁷⁸ Omdat echter de verstoringsopdracht – zoals omschreven in het ontwerp van art. 7, 5° en art. 11, 7° – zeer ruim is en geen concrete maatregelen bevat, vloeit hieruit voort dat ook de reikwijdte van betrokken vorderingsbevoegdheid quasi weinig begrensd wordt. Zeker wanneer een dergelijke medewerking gepaard gaat met het plegen van strafbare inbreuken is dit problematisch in het licht van het legaliteitsbeginsel in strafzaken.

89. De schriftelijke vraag van de betrokken inlichtingendienst tot akkoord van de BIM-Commissie om een vordering tot medewerking te richten in het kader van een uitzonderlijke methode moet een aantal verplichte vermeldingen bevatten (cf. ontwerp art. 18/10, §3/2, tweede lid). Een van de vermeldingen is *“het ernstig gevaar voor de fysieke integriteit van één of meer personen of in het kader van activiteiten verband houdend met terrorisme of criminele organisaties”* (punt 3°). Het Comité stelt vast dat een vergelijkbare inhoudelijke motivering ontbreekt in de schriftelijke vraag van de betrokken inlichtingendienst tot akkoord van de BIM-Commissie om een vordering tot medewerking te richten in het kader van een verstoringsopdracht (cf. ontwerp art. 19/6, §2, tweede lid). Het Comité is van oordeel dat eenzelfde vermelding moet toegevoegd worden (ADV-65). In het licht van het advies over de verstoringsopdracht kan dit als volgt omschreven worden: *“de ernstige en actuele dreiging voor de nationale veiligheid”*.

⁷⁸ Memorie van toelichting, pag. 79.



Strafbaarstellingen en bijhorende strafsancties

90. Het ontwerp paragraaf 3/4 van art. 18/10 WIV en het ontwerp paragraaf 5 van art. 19/6 WIV bevatten de strafbaarstelling en de bijhorende strafsanctie voor de personen die hun medewerking weigeren te verlenen.

Ontwerp art. 18/10, §3/4:

“Eenieder die zijn medewerking weigert te verlenen aan de in paragraaf 3/1 tot en met paragraaf 3/3 bedoelde vorderingen wordt bestraft met een straf van niveau 1.”.

Ontwerp art. 19/6, §5:

“Eenieder die zijn medewerking weigert te verlenen aan de in paragraaf 1 tot en met paragraaf 3 bedoelde vorderingen wordt bestraft met een straf van niveau 1.

In afwijking van het eerste lid, wordt elke natuurlijke persoon of rechtspersoon waarvan de medewerking kan gevorderd worden voor de uitvoering van de methoden bedoeld in art. 18/2, §1 en §2 en die zijn medewerking weigert te verlenen aan de in paragraaf 1 tot en met paragraaf 3 bedoelde vorderingen, bestraft met een straf van niveau 2. In afwijking van artikel 52 van het Strafwetboek, bedraagt de geldboete als bijkomende straf ten minste 200 euro en ten hoogste 160.000 euro.”.

De memorie van toelichting bevat geen verduidelijking aangaande beide bepalingen. Het Comité is van oordeel dat hier nochtans een nood toe bestaat (ADV-66). Wat betreft ontwerp art. 18/10, §3/4 is het onduidelijk wat de verhouding is tussen de hierin bepaalde strafbaarstelling en strafsanctie en de bestaande strafbaarstellingen en strafsancties bepaald ten opzichte van postoperatoren (art. 18/14, §3 WIV), operatoren van elektronische communicatienetwerken en verstrekkers van elektronische communicatiediensten (art. 18/17, §3, tweede lid WIV), bepaalde financiële instellingen (art. 18/15, §4 WIV), en bepaalde deskundigen in informaticasystemen en -diensten (art. 18/16, §4 WIV), te meer gezien het wetsontwerp laatstgenoemde strafsancties verzwaard (zie art. 48 wetsontwerp). Deze laatste maatregel wordt verantwoord, volgens het Comité terecht, door een gelijkschakeling met het misdrijf “miskenning van de plicht tot medewerking aan het (straf)onderzoek” (art. 655 SW-2024). Het Comité adviseert om deze verhouding in de memorie van toelichting te verduidelijken.

Wat betreft ontwerp art. art. 19/6, §5 is het toepassingsgebied van het tweede lid hoogst onduidelijk. Deze stelt: *“In afwijking van het eerste lid,”* – dit lid handelt over de weigering medewerking te verlenen aan een verstoringsactie – *“wordt elke natuurlijke persoon of rechtspersoon waarvan de medewerking kan gevorderd worden voor de uitvoering van de methoden bedoeld in art. 18/2, §1 en §2”* – dit zinsdeel handelt over de medewerking te verlenen in het kader van uitzonderlijke én specifieke inlichtingenmethoden – *“en die zijn medewerking weigert te verlenen aan de in paragraaf 1 tot en met paragraaf 3 bedoelde vorderingen, bestraft met (...)”.* Het Comité adviseert om deze bepaling ofwel te schrappen ofwel te herschrijven en te verduidelijken in de memorie van toelichting (ADV-67).

Tarieven

91. Het Comité stelt zich voorts de vraag of art. 18/18 WIV, dat handelt over de tarieven die door de betrokken inlichtingendienst moet betaald worden voor de medewerking van derden, ook van toepassing is op de medewerking zoals bedoeld in ontwerp art. 18/10, §3/1 ev. WIV. Dit lijkt zo te zijn gezien betrokken bepalingen deel uitmaken van onderdeel 2. Art. 18/18 WIV stelt namelijk: *“De Koning legt de tarieven vast voor de medewerking van de natuurlijke personen en rechtspersonen aan de methoden bedoeld in artikel 16/2 en in de onderafdeling 2, waarbij Hij rekening houdt met de werkelijke kostprijs van deze medewerking.”.* Het Comité kon



hierover niets terugvinden in de memorie van toelichting en vraagt dit uit te klaren. Tevens wordt gevraagd aan de regering of bestaand KB van toepassing is of als hiervoor een nieuw KB dient ingesteld te worden (ADV-68).

Aangezien ontwerp art. 19/6 WIV geen deel uitmaakt van onderafdeling 2, afdeling 4, hoofdstuk 3 van de Inlichtingenwet kan besloten worden dat art. 18/18 WIV geen toepassing kent voor wat betreft de medewerking van derden in het kader van verstoring. Desondanks adviseert het Comité om ook over deze kwestie een aparte regeling rond te voorzien (ADV-69).

(12) BESCHERMDE BEROEPSCATEGORIEËN

92. Het wetsontwerp schrapt de verplichte kennisgeving van de BIM-Commissie aan de voorzitter van de Ordes van advocaten⁷⁹, van de Orde van artsen en van de Vereniging van beroepsjournalisten voorafgaand aan een geplande specifieke of uitzonderlijke methode (schrapping van art. 18/2, §3 en invoeging van nieuw art. 18/2/1, §3). De memorie van toelichting verantwoordt deze maatregel door te stellen dat *“(d)eze kennisgeving (...) geen inhoudelijke component (heeft): de voorzitter van de beroepsvereniging heeft geen enkele beoordelingsbevoegdheid, noch de bevoegdheid om tegen de aanwending van de methode op te treden”*. Tevens wordt gesteld *“(h)oewel de voorgestelde wijziging de geldende bepalingen en procedures efficiënter en soepeler maakt, wordt er niet geraakt aan de garanties die worden geboden ter bescherming van de gegevens van een advocaat, een arts of een journalist die vallen onder het beroeps- of bronnengeheim”*.⁸⁰ Het Comité adviseert om advies in te winnen bij vernoemde Ordes en Vereniging om na te gaan of dit motief effectief is (ADV-70).

93. Binnen de bijzondere procedure van toepassing bij het inwinnen van informatie van specifieke en uitzonderlijke methoden rijst wel de vraag hoe de voorzitter van de BIM-Commissie kan weten welke van de reeds ingewonnen informatie onder de toepassing van het beroepsgeheim valt en welke niet. Betrokken procedure stelt immers dat *“de voorzitter van de commissie of, bij verhindering, een ander Commissielid (gaat) na of de via deze methode verkregen gegevens een rechtstreeks verband hebben met de potentiële dreiging, wanneer zij beschermd worden door het beroepsgeheim van een advocaat of arts of door het bronnengeheim van een journalist”*.

Art. 90octies, §3 Sv., die een vergelijkbare procedure binnen het strafrechtelijk vooronderzoek bevat, lost deze vraagstelling op door de onderzoeksrechter de verplichting op te leggen, voor dit doel, overleg te plegen met de Orde van advocaten of de Orde van artsen. Het is aanbevelenswaardig om eenzelfde regeling in te voeren, zeker wanneer de voorafgaande kennisgevingsplicht wordt geschrapt (ADV-71).

(13) GEHEIMHOUDINGSPLICHT (art. 36 WIV)

94. Het wetsontwerp breidt de geheimhoudingsplicht uit naar personen *“aan wie wordt gevraagd zijn medewerking te verlenen”*. Deze wijziging is volgens het Comité met afdoende redenen omkleedt. Wel stelt het Comité zich de vraag bij §2 van art. 36 of het toepassingsgebied – naast uitgebreid wat betreft vernoemde personen – doelbewust wordt beperkt voor wat betreft de agenten van de inlichtingendiensten.

Huidig art. 36, §2 stelt:

⁷⁹ M.n. de Orde van de Vlaamse balies en de Ordre des barreaux francophones et germanophone.

⁸⁰ Memorie van toelichting, pag. 11.



“Het geheim blijft bestaan zelfs wanneer de agenten hun functie hebben neergelegd of de personen hun medewerking met de diensten hebben stopgezet.”

Het voorgestelde art. 36, §2 stelt:

“Het geheim blijft bestaan zelfs wanneer de agent of de persoon bedoeld in paragraaf 1 zijn medewerking heeft stopgezet of weigert zijn medewerking te verlenen.”.

Zodoende worden de woorden “hun functie hebben neergelegd” geschrapt. Dit is een beperking van het toepassingsgebied van art. 36, §2. Via deze weg worden eveneens de strafrechtelijke inbreuken in art. 43 WIV beperkt gelet op de verwijzing aldaar naar “de agent of de persoon bedoeld in artikel 36”.

Het Comité vraagt om ofwel in de memorie van toelichting te verduidelijken waarom betrokken toepassingsgebied wordt beperkt, ofwel betrokken schrapping weg te laten (ADV-72).

(14) KENNISGEVING NIET-INWONENDE PARTNER VEILIGHEIDSONDERZOEK (ontwerp art. 16, §4 WCV)

95. Het Comité R/I stelt vast dat in uitvoering van zijn DPA-beslissing VCI/DPA/2026/01 van 3 februari 2026 in verband met een nieuwe basisvragenlijst van de VSSE, voorzien wordt in een duidelijke wettelijke regeling voor individuele veiligheidsonderzoeken op de niet-samenwonende partner(s) van een persoon die een veiligheidsmachtiging behoeft en waarmee deze laatste een duurzame relatie heeft. Het Comité is van oordeel dat deze bepaling zo goed als mogelijk de veiligheidsbelangen verzoent met de bescherming van de privacy van derden. Wel merkt het Comité op dat indien de term ‘duurzame relatie’ (uitsluitend) zou gedefinieerd worden in een richtlijn van de Nationale Veiligheidsraad in uitvoering van artikel 18, vijfde lid, Classificatiewet van 11 december 1998 (zoals aangekondigd in de Memorie van Toelichting), deze niet tegenstelbaar is aan de betrokkene, diens ‘partner’, de Raad van State (bijv. bij een beslissing om de aanvraag van een veiligheidsonderzoek onontvankelijk te verklaren) of aan het Beroepsorgaan inzake veiligheidsmachtigingen en veiligheidsadviezen (bijv. bij een weigering of intrekking van een veiligheidsmachtiging gelieerd omwille van feiten gelieerd aan een partner). Immers, dergelijke richtlijnen zijn ingevolge die wettelijke bepaling niet openbaar. Het Comité beveelt aan om de termen ‘partner’ en ‘duurzame relatie’ in de wet, de Memorie van Toelichting of in een openbare richtlijn te definiëren zodat in eerste instantie elke betrokkene zo goed als mogelijk op voorhand kan bepalen wat de mogelijke gevolgen zijn van het aangaan van een bepaalde relatie voor een veiligheidsmachtiging (ADV-73). Dit is zeker van belang wanneer er een ‘buitenlandse component’ speelt (wonen of gewoond hebben in het buitenland of andere nationaliteit hebben) omdat dit directe gevolgen kan hebben voor een aanvraag tot een veiligheidsmachtiging.

(15) WETGEVENDE TUSSENKOMST VEREIST – OPENBAARHEID VAN BESTUUR

96. Het Comité herinnert de opsteller aan het arrest van het Grondwettelijk Hof waarbij de actieve kennisgevingsplicht in art. 2, §3 WIV werd vernietigd (*infra*), en waar de wetgever vooralsnog heeft nagelaten deze te herstellen. Een dergelijke verplichting, ook wel gekend als de ‘(actieve) notificatieplicht’, houdt in dat de VSSE en de ADIV onder bepaalde voorwaarden uit eigen beweging een geviseerde persoon op de hoogte moeten brengen dat hij of zij het voorwerp van onderzoek is geweest, meer in het bijzonder dat in het verleden een bepaalde inlichtingenmethode op hem of haar werd toegepast. Anders gesteld, een actieve notificatieplicht betekent dat een inlichtingendienst ambtshalve haar onderzoek en informatiepositie ten aanzien van een (voormalig) geviseerde deels moet kenbaar maken.



Bij Wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten (kortweg: BIM-wet) werd voor de eerste maal een actieve kennisgevingsplicht in hoofde van de VSSE en de ADIV ingesteld. Betrokken artikel 2, §3 WIV werd echter in 2011 vernietigd door het Grondwettelijk Hof (nr. 145/2011). Bij 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 (kortweg: BIM-actualisatiewet) werd voor de tweede maal een dergelijke notificatieplicht wettelijk ingesteld. Betrokken artikel 2, §3 WIV werd evenwel, in 2019, opnieuw door het Grondwettelijk Hof vernietigd (nr. 41/2019). Het Comité beveelt aan om betrokken regeling te herstellen en hierbij rekening te houden met de rechtspraak van het Grondwettelijk Hof (ADV-74).

97. Het Comité herinnert de opsteller eveneens aan art. 7, §3 Classificatiewet dat stelt: “*De bevoegde controleorganen van de overheid van oorsprong worden door de Koning bepaald.*”. Bij Wet van 7 april 2023⁸¹ werd in de Classificatiewet een algemene declassificatieregeling ingevoerd. In de wet werden periodes voorzien waarbij de overheden van oorsprong – dus de classificerende instanties – verplicht worden na te gaan of de classificatie en het classificatieniveau nog dient gehandhaafd te worden. Betrokken wetsartikel stelt: “*Bij ontstentenis van een evaluatie binnen tien jaar kan het bevoegde controleorgaan de overheid van oorsprong schriftelijk bevelen om binnen drie maanden de classificatie te evalueren overeenkomstig het eerste tot het derde en het achtste tot het tiende lid. Indien de evaluatie niet plaatsvindt binnen drie maanden na dit schriftelijk bevel, vervalt de classificatie.*”. In zijn wetgevingsadvies van 22 juli 2024 aangaande het ontwerp van KB tot uitvoering van de Classificatiewet stelt het Comité: “*Het Comité beveelt aan in dit besluit uitvoering te geven te geven aan artikel 7 §3 dat de Koning oplegt de bevoegde controleorganen aan te duiden dat moet optreden in het kader van evaluaties opgesteld door de overheid van oorsprong bij een eventuele declassificatie of verlenging van de classificatietermijn.*”.⁸² Het Comité stelt vast dat hieraan geen gevolg werd gegeven. Het Comité beveelt aan om betrokken wetsbepaling te wijzigen en rechtstreeks in de wet de bevoegde controleorganen aan te duiden (ADV-75).

(16) TAALKUNDIGE OPMERKINGEN M.B.T. DE INLICHTINGENWET

98. Het begrip “Directeur Operaties VSSE” (ADV-76). Art. 3, 18° WIV omschrijft de “Directeur Operaties van de Veiligheid van de Staat” als “*de agent van de buitendiensten van de Veiligheid van de Staat, bekleed met de graad van commissaris-generaal, die belast is met de leiding van de buitendiensten van de Veiligheid van de Staat*”. In het licht van het KB van 18 augustus 2025 houdende diverse bepalingen betreffende de leden van het directiecomité van de Veiligheid van de Staat (BS 22 augustus 2025) correspondeert deze bepaling niet meer met de reglementaire organisatie van de VSSE. Indachtig de in dit KB toegewezen bevoegdheden wordt het begrip “Directeur Operaties van de Veiligheid van de Staat” best vervangen door het begrip “Directeur Operationele Inlichtingen van de Veiligheid van de Staat”. De omschrijving kan hierbij eveneens best vervangen worden als “*de agent van de Veiligheid van de Staat, die belast is met de leiding van de directie Operationele Inlichtingen van de Veiligheid van de Staat zoals door de Koning bepaalt*”. Een dergelijke omschrijving houdt meer rekening met de mandaatfunctie van betrokken hoedanigheid, alsook met de soort personeelsleden onder het gezag en leiding van betrokkene.

99. De naam van de Wet van 11 december 1998 (ADV-77). Sinds de wet van 2 juni 2024 (BS 8 juli 2024) is de correcte benaming, de “wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst”. De Wet van 30 november 1998 bevat diverse

⁸¹ Wet van 7 april 2023 houdende wijziging van de wet van 11 december 1998, betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (BS 9 juni 2023).

⁸² Advies nr. 008/VCI-BTA/2024 van 22 juli 2024 betreffende het ontwerp van koninklijk besluit tot uitvoering van de Classificatiewet van 11 december 1998, pag. 9.



bepalingen die aan niet zijn aangepast aan de nieuwe naam (m.n. art. 13, §4, art. 18/17, §5, art. 21/1, §3, art. 43/1, §2, en art. 43/5, §3).

(17) INLICHTINGENMETHODEN: CREATIE VAN EEN JURIDISCH KADER VOOR EEN TEST-OMGEVING

100. Het wetsontwerp voorziet in een testomgeving (sandbox) voor handelingen die verband houden met artificiële intelligentie (*supra*). Het zou coherent zijn om ook te voorzien in een wettelijk kader voor een testomgeving gewijd aan BIM-methoden, gezien hun technische complexiteit en hun potentiële impact op de grondrechten. Een dergelijk mechanisme zou het mogelijk maken om BIM-methoden te testen, te evalueren en te omkaderen vóór de operationele uitrol ervan.

Daarnaast schaffen de inlichtingendiensten regelmatig nieuwe apparatuur aan. Ook worden er trainingen gegeven voor de gewone methodes, waarbij echte persoonsgegevens worden verzameld (bijvoorbeeld tijdens HUMINT-training). Er bestaat rechtsonzekerheid over de wijze waarop deze trainingen moeten worden behandeld. De criteria inzake dreiging, proportionaliteit of subsidiariteit kunnen niet worden toegepast. Het Comité stelt voor om een ondersteuningsmaatregel in te voeren waarbij de BIM-Commissie en het Comité vooraf op de hoogte worden gesteld van de oefeningen en tests en waarbij de verzamelde gegevens onmiddellijk en systematisch worden vernietigd na de oefening of de test (ADV-78).

(18) TOEZICHTMODALITEITEN

101. Het Comité is een onafhankelijke instelling. Deze onafhankelijkheid en het effectieve karakter van het toezicht zijn voorwaarden die als essentieel zijn erkend voor de grondwettelijkheid van de normen waarop het Comité I toezicht houdt (zie de arresten nrs. 145/2011, 41/2019, 27/2020 en 134/2025 van het Grondwettelijk Hof).

De uitbreiding van de actie- en collectemiddelen van de inlichtingendiensten moet uiteraard gepaard gaan met een uitbreiding van de bevoegdheden van de machtigings- en toezichtsautoriteiten, te weten de BIM-commissie en het Comité. In de loop der jaren zijn de bevoegdheden toegenomen⁸³ en de modaliteiten voor de uitoefening ervan variëren sterk. Dit resulteert in een veelvoud aan verschillende processen die moeilijk te implementeren zijn met de technische en personele middelen van het Comité. Deze uitbreiding van de middelen van de diensten, en het uitvloeisel daarvan in de vorm van de toevoeging van uiteenlopende bevoegdheden aan het Comité, ging niet gepaard met een structurele herziening van de controle-instrumenten en de toekenning van de capaciteit om op eenvoudige en directe wijze informatie te verkrijgen die relevant is voor een of meer (eventueel transversale) controles. Met andere woorden: de veelheid aan bevoegdheden en de manieren om deze uit te oefenen, maken het toezicht van het Comité complex. Om die redenen acht het Comité structurele en transversale maatregelen noodzakelijk om een effectief toezicht op de inlichtingendiensten te behouden.

102. In dat opzicht beveelt het Comité aan om de Wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten te wijzigen om er verschillende bepalingen in op te nemen. Deze in bijlage gepresenteerde wijzigingen versterken de democratische legitimiteit van de inlichtingendiensten door

⁸³ Met name het toezicht door middel van onderzoeken of de behandeling van klachten op de wettelijkheid, de doeltreffendheid en de coördinatie; de rol van gegevensbeschermingsautoriteit; de behandeling van meldingen van inbreuken op de integriteit; het toezicht achteraf (a posteriori) op de bijzondere methoden voor het verzamelen van gegevens; het toezicht op bepaalde gewone maatregelen en op de beschermings- en ondersteuningsmaatregelen, enz.



een effectieve auditeerbaarheid mogelijk te maken. Hierdoor worden de verantwoordelijke politieke autoriteiten en het publiek gerustgesteld over het respect voor de grondrechten, met behoud van hun operationele doeltreffendheid. (ADV-79).

Brussel, 3 juni 2026

VOOR HET COMITÉ R/I

Vanessa SAMAIN
Voorzitster

Frédéric GIVRON
Griffier