Bijlage B

bij het Toezichtsrapport over de toepassing van filters bij OOG-interceptie door de AIVD en de MIVD

CTIVD nr. 63

[vastgesteld op 17 juli 2019]

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Leeswijzer

Het rapport bestaat uit verschillende delen:

Het Toezichtsrapport
Bijlage A: Verdieping op het Toezichtsrapport
Bijlage B: Toetsingskader
Bijlage C: Begrippenlijst

Dit rapport heeft een geheime bijlage.

Vanwege de (technische) complexiteit van het onderwerp heeft de CTIVD ervoor gekozen het rapport op te delen in een Toezichtsrapport met de belangrijkste bevindingen en een separate Bijlage (A), die op een hoger detailniveau op de bevindingen ingaat. Voor een verdieping in het onderwerp verdient het daarom aanbeveling Bijlage A te lezen. Het Toezichtsrapport en Bijlage A zijn geschreven als zelfstandig leesbare stukken en bevatten daarom onvermijdelijk enige overlap. Het volledige Toetsingskader is ondergebracht in Bijlage B. Bijlage C is de Begrippenlijst.

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 63

BIJLAGE B: TOETSINGSKADER

bij het Toezichtsrapport over de toepassing van
filters bij OOG-interceptie door de AIVD en de MIVD

Inhoudsopgave

B.1 Inleiding 3

B.2 Het driefasenmodel van OOG-interceptie 4

2.1 Interceptie 4

2.2 Optimalisatie van het interceptieproces 5

2.3 Analyse van gegevens 7

B.3 Filters 8

3.1 Wat is filteren? 8

3.2 Filteren in het driefasenmodel 8

B.4 Vereisten voor de toepassing van filters in het kader van OOG-interceptie 11

4.1 Taakstelling en onderzoeksopdrachten 11

4.2 Zo gericht mogelijk 11

4.3 Datareductie 12

4.4 Kabelinterceptie 13

4.5 Overige invloeden op het toepassen van de filters 14

4.6 Interne controle en effectief toezicht 16

CTIVD nr. 63

BIJLAGE B: TOETSINGSKADER

bij het Toezichtsrapport over de toepassing van filters bij OOG-interceptie door de AIVD en de MIVD

B.1 Inleiding

Dit diepteonderzoek naar de toepassing van filters bij de inzet van onderzoeksopdrachtgerichte (OOG-) interceptie komt voort uit de resultaten van de voortgangsrapportage die de CTIVD in december 2018 heeft gepresenteerd. Daarin concludeert de CTIVD dat filtering bij etherinterceptie in de praktijk van de diensten plaatsvindt, maar dat deze praktijk niet in beleid, werkprocessen of -instructies is beschreven. De CTIVD heeft aangegeven dat onder andere deze constateringen leiden tot de conclusie dat er sprake is van hoge risico's voor onrechtmatig handelen door beide diensten.

Door middel van dit (kortlopend) diepteonderzoek kan een beeld worden verkregen van de toepassing van filters door de diensten, waarna een rechtmatigheidstoets kan plaatsvinden aan de hand van dit toetsingskader. Met dit onderzoek wordt dus beoordeeld of de geconstateerde risico's zich ook hebben gemanifesteerd. Dit onderzoek richt zich naast ether- ook op (de voorbereidingen voor) kabelinterceptie, omdat de nieuwe bevoegdheid tot bulkinterceptie op de kabel in aanloop naar de inwerkingtreding van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017) tot groot maatschappelijk debat heeft geleid. De wijze van filtering kan per interceptietechniek verschillen; bijzonderheden worden dan ook specifiek benoemd.

De noodzaak voor een rechtmatigheidstoets met betrekking tot filteren vloeit niet alleen voort uit eerdergenoemde constateringen, maar ook uit de wetsgeschiedenis en jurisprudentie. Zo worden filters in de wetsgeschiedenis aangehaald als instrument om de inbreuk op fundamentele rechten en vrijheden door de inzet van onderzoeksopdrachtgerichte interceptie te mitigeren en onderstreept het *Big Brother Watch*-arrest van het EHRM de noodzaak van effectief onafhankelijk toezicht op de toepassing van filters in het proces van bulkinterceptie.

Het toetsingskader voor het onderzoek naar de toepassing van filters bij OOG-interceptie is als volgt opgebouwd. Hoofdstuk 2 geeft een beschrijving van het proces van OOG-interceptie. In hoofdstuk 3 wordt de toepassing van filters in het interceptieproces toegelicht. In hoofdstuk 4 worden ten slotte de vereisten geformuleerd die aan de filters dienen te worden gesteld, zoals deze voor de AIVD en de MIVD volgen uit de Wiv 2017 (inclusief wetsgeschiedenis) en jurisprudentie.

B.2 Het driefasenmodel van OOG-interceptie

In dit hoofdstuk wordt het OOG-interceptiestelsel toegelicht aan de hand van de drie fasen die in de memorie van toelichting op de Wiv 2017 zijn geformuleerd.[1] De memorie van toelichting bevat veel informatie over de voorwaarden van de inzet en de reikwijdte van de bijzondere bevoegdheden met betrekking tot OOG-interceptie. Helderheid over het juridisch kader komt de rechtszekerheid van de betrokkenen ten goede en verschaft handvatten aan de toezichthouder.

Het onderscheid in drie fasen is voornamelijk juridisch van aard, omdat in de praktijk de fasen continu plaatsvinden en elkaar voortdurend onderling beïnvloeden.[2] Dat blijkt ook uit de aanvragen tot de inzet van de desbetreffende bijzondere bevoegdheden in art. 48-50 Wiv 2017. In de praktijk wordt één gecombineerde aanvraag gedaan met betrekking tot de interceptie en optimalisatie daarvan (art. 48 jo 49 lid 1 Wiv 2017) en één gecombineerde aanvraag met betrekking tot selectie en de optimalisatie daarvan (art. 49 lid 2 jo art. 50 lid 1 sub a Wiv 2017). Dit wordt tevens geïllustreerd door het feit dat de diensten in hun beleid en praktijk vijf fasen, in plaats van drie, hanteren.

De drie fasen betreffen kort gezegd (1) de interceptie van communicatie, (2) de optimalisatie van het interceptieproces en (3) de analyse van de inhoud van de communicatie en metadata (gegevens over de communicatie).

2.1 Interceptie

Met de naam van de bijzondere bevoegdheid 'onderzoeksopdrachtgerichte interceptie van communicatie' vindt nadrukkelijk een koppeling met de Geïntegreerde Aanwijzing inlichtingen- en veiligheidsdiensten plaats. De Geïntegreerde Aanwijzing wordt vastgesteld door de minister-president, minister van Algemene Zaken, de minister van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK) en de minister van Defensie en vormt de basis voor de onderzoeksopdrachten van de diensten. Daarnaast kan er sprake zijn van acute onderzoeksopdrachten die ook op ministerieel niveau worden geaccordeerd.[3] Nadat de Geïntegreerde Aanwijzing is vastgesteld, worden door de diensten onderzoeksopdrachten opgesteld aan de hand van de toepasselijke wettelijke taak, waarin het doel en de noodzaak van het onderzoek is vastgelegd. In de memorie van toelichting wordt als voorbeeld van een onderzoeksopdracht het verwerven van telecommunicatie in een missiegebied en het verwerven van metadata tussen gebieden in handen van terroristen en Nederland.[4] Onderzoeksopdrachten zien alleen op de uitvoering van de taken van de AIVD en de MIVD. De bijzondere bevoegdheid van OOG-interceptie mag daarbij alleen worden uitgevoerd in het kader van de inlichtingen- en veiligheidstaken.[5]

De eerste fase van het OOG-interceptiestelsel bestaat uit de interceptie van communicatie ter uitvoering van de onderzoeksopdrachten.[6] De bijzondere bevoegdheid tot de interceptie zelf is neergelegd in artikel 48 Wiv 2017. De bevoegdheid omvat ook het ongedaan maken van de versleuteling van telecommunicatie of gegevensoverdracht en de technische analyse van de gegevens, voor zover deze gericht is op de optimalisatie van de uitoefening van de interceptiebevoegdheid.

1 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 96-109.
2 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 96.
3 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 90.
4 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 95.
5 Meer specifiek met betrekking tot de uitvoering van art. 8 lid 2 sub a en d en art. 10 lid a, c en e Wiv 2017 (zie art. 28 lid 1 Wiv 2017).
6 Meer juridisch geformuleerd betreft het de bevoegdheid met een technisch hulpmiddel onderzoeksopdrachtgericht af te tappen, te ontvangen, op te nemen en af te luisteren van elke vorm van telecommunicatie of gegeven overdacht door middel van een geautomatiseerd werk, ongeacht waar een en ander plaatsvindt.

De inhoud van de communicatie mag bij de technische analyse uitsluitend worden gecontroleerd op de goede uitlevering van de ontvangst (een kwaliteitscontrole), bijvoorbeeld of de communicatie bestaat uit ruis.[7]

Wanneer de diensten overtuigd zijn van het doel en de noodzaak, proportionaliteit en subsidiariteit van de inzet, zal toestemming worden gevraagd aan de minister van BZK en/of de minister van Defensie om de gevraagde vorm van OOG-interceptie uit te mogen voeren voor een periode van maximaal één jaar. Met de inwerkingtreding van art. 5 van de Beleidsregels Wiv 2017 dient in het verzoek om toestemming nadrukkelijk te worden aangegeven op welke wijze de toepassing van bijzondere bevoegdheden zo gericht mogelijk plaatsvindt (zie verder hoofdstuk 4).[8]

In de aanvraag tot interceptie moet een typering worden gegeven van de telecommunicatie of de gegevensoverdracht door middel van een geautomatiseerd werk ten aanzien waarvan de bevoegdheid dient te worden uitgeoefend. Uit de aanvraag moet blijken om welke vorm van interceptie het gaat: interceptie van etherverkeer of kabelgebonden verkeer. Ook moet, voor zover mogelijk, de aard van het verkeer, zoals GSM-, radio- of internetverkeer, worden aangegeven in combinatie met een geografische afbakening. Bovendien nemen de AIVD en de MIVD in hun aanvraag op welke soorten verkeer relevant zijn, zoals spraak, chatverkeer of bestandsuitwisseling. Bij interceptie op kabelgebonden verkeer moet worden aangegeven welk deel van de kabelinfrastructuur het betreft en wat voor verkeer dient te worden geïntercepteerd.[9] Ten behoeve van de keuze op welk punt van de infrastructuur de diensten de interceptiebevoegdheid willen inzetten, kunnen de diensten informatie opvragen bij aanbieders van communicatiediensten. Deze aanbieders hebben een medewerkingsplicht om deze informatie te verschaffen en medewerking te verlenen om interceptie mogelijk te maken.[10] De diensten kiezen datastromen uit waarvan de gerede verwachting bestaat dat ze relevant zijn voor het beantwoorden van de onderzoeksopdrachten van de diensten.[11]

Op grond van art. 48 lid 3 Wiv 2017 geldt een extra motiveringseis als niet met de interceptie van louter metadata kan worden volstaan. Slechts speciaal geautoriseerde medewerkers mogen kennisnemen van de gegevens ten behoeve van het ongedaan maken van versleuteling en in het kader van technische analyse controleren van de goede uitvoering van de ontvangst (inclusief de inhoud van communicatie).

Na verkregen toestemming van de desbetreffende minister wordt de aanvraag tot de inzet van de bijzondere bevoegdheid voorgelegd aan de Toetsingscommissie Inzet Bevoegdheden (TIB). Als de TIB van oordeel is dat de toestemming rechtmatig is gegeven, kan de interceptie aanvangen.

2.2 Optimalisatie van het interceptieproces

De tweede fase van het OOG-interceptiestelsel heeft tot doel het optimaliseren van de opbrengst van de interceptie (‘*search gericht op interceptie*’, geregeld in art. 49 lid 1 Wiv 2017) en de optimalisatie van het navolgende selectieproces (‘*search gerichte op selectie*’, art. 49 lid 2 Wiv 2017).[12] In deze fase gaat het in eerste instantie niet om kennisneming van gegevens, maar om het verzamelen van informatie waarmee in het bijzonder het interceptieproces in bredere zin kan worden geoptimaliseerd.

7 Zie *Kamerstukken II* 2016/17, 34588, nr. 3, p. 97-103 (onder de kop ‘fase 1’).
8 Beleidsregels Wiv 2017.
9 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 99.
10 Artikel 52 Wiv 2017 (informatie) en artikel 53 Wiv 2017 (medewerking).
11 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 110.
12 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 95.

2.2.1 Search gericht op interceptie

Bij search gericht op interceptie gaat het om de verkenning van de telecommunicatie. De bijzondere bevoegdheid in art. 49 lid 1 Wiv 2017 strekt ertoe om het gebruik van telecommunicatienetwerken te verkennen door het vaststellen van de kenmerken en de aard van de telecommunicatie, alsmede de identiteit van de persoon of organisatie die bij een telecommunicatie hoort. Deze vorm van search is primair gericht op de optimalisatie van interceptie, waarbij vooral naar de aard van het verkeer wordt gekeken. Daaronder valt bijvoorbeeld ook het herkennen van de taal van de communicatie. In veel gevallen wordt dit proces uitgevoerd door geautomatiseerde processen. Search gericht op interceptie ziet vooral op de technische kenmerken en de aard van de communicatie, zoals protocollen, frequenties, taal en de kwaliteit van de intercepties.[13]

Voor de uitoefening van de bevoegdheid is op grond van artikel 49 lid 4 Wiv 2017 toestemming vereist van de voor de desbetreffende dienst verantwoordelijke minister. Deze toestemming kan worden verleend voor de periode van een jaar, met de mogelijkheid deze telkens met een jaar te verlengen. Zoals in de inleiding van dit hoofdstuk is opgemerkt, betreft het in de praktijk een combinatielast van artikel 48 en 49 lid 1 Wiv 2017.

2.2.2 Search gericht op selectie

Search gericht op selectie heeft te maken met de optimalisatie van selectie bij het OOG-interceptiestelsel. Deze bijzondere bevoegdheid is geregeld in artikel 49 lid 2 Wiv 2017. Bij de uitoefening van deze bevoegdheid gaat het ten eerste om het vaststellen van en verifiëren van selectiecriteria in relatie tot personen en organisaties die door de diensten worden onderzocht. In de opbrengst van de geïntercepteerde telecommunicatie kan dan op zoek worden gegaan naar selectiecriteria die – op grond van artikel 50 lid 3 vastgesteld – voor het onderzoek van de diensten naar personen of organisaties relevante gegevens kunnen opleveren. Daarnaast kunnen potentiële selectiecriteria op hun bruikbaarheid worden geverifieerd, door in de opbrengst van de geïntercepteerde telecommunicatie te bezien of deze relevante gegevens voor het onderzoek opleveren.[14]

De bijzondere bevoegdheid in artikel 49 lid 2 Wiv 2017 maakt het ook mogelijk - in relatie tot lopende onderzoeken - personen of organisaties te identificeren die in aanmerking komen voor onderzoek van de AIVD of de MIVD.[15] De bijzondere bevoegdheid verschaft met andere woorden ook de mogelijkheid potentiële targets te identificeren of te duiden.[16] Aan de hand van gegevens uit lopende onderzoeken kan worden nagegaan of middels de opbrengst van de geïntercepteerde telecommunicatie aan die gegevens personen of organisaties zijn te koppelen die mogelijk voor onderzoek van de AIVD of MIVD in aanmerking komen. Als bij het searchen de opbrengst van de telecommunicatie nieuwe targets of organisaties worden onderkend die in aanmerking komen voor onderzoek door de AIVD of de MIVD, dan moet voor het gebruik van de inhoud van de communicatie toestemming als bedoeld in artikel 50 lid 2 Wiv 2017 worden verkregen.[17]

Voor de inzet van de bijzondere bevoegdheid in artikel 49 Wiv 2017 is toestemming van de voor de desbetreffende dienst verantwoordelijke minister vereist. Een gegeven toestemming geldt voor de duur van drie maanden. Slechts speciaal aangewezen ambtenaren mogen op grond van art. 49 lid 5 Wiv 2017 kennisnemen van de opgeslagen inhoud uit OOG-interceptie (functie- en/of taakscheiding). In artikel 49 lid 3 Wiv 2017 staat dat van de resultaten van het onderzoek in artikel 49 Wiv 2017 aantekening mag worden gehouden, indien dat noodzakelijk is voor de goede taakuitvoering van de diensten.

13 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 104.
14 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 106. Zie ook CTIVD-rapport nr. 28 (2011), p. 43.
15 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 107.
16 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 106. Zie ook CTIVD-rapport nr. 28 (2011), p. 44.
17 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 107.

2.3 Analyse van gegevens

In de derde fase van het OOG-interceptiestelsel vindt de selectie van relevante communicatie plaats met het oogmerk om van de *inhoud* van de geselecteerde gegevens kennis te kunnen nemen.[18] De bevoegdheid om selectie toe te passen op de geïntercepteerde gegevens is vastgelegd in art. 50 lid lid 1 sub a Wiv 2017.

Tevens vindt in deze derde fase van het OOG-interceptieproces metadata-analyse plaats, welke gericht kan zijn op het identificeren van personen of organisaties. Deze onderzoeksactiviteit is genormeerd door de bijzondere bevoegdheid van geautomatiseerde data-analyse in art. 50 lid 1 sub b Wiv 2017, en art. 50 lid 4 voor zover het metadata betreft die afkomstig zijn uit OOG-interceptie en de analyse gericht is op het identificeren van personen of organisaties.

18 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 107.

B.3 Filters

In dit hoofdstuk wordt nader geduid wat onder een filter moet worden verstaan en hoe de toepassing van filters moet worden geplaatst in het in het vorige hoofdstuk toegelichte driefasenmodel.

3.1 Wat is filteren?

In dit onderzoek naar de toepassing van filters tijdens het proces van OOG-interceptie wordt een filter gedefinieerd als het middel dat bepalend is voor het al dan niet (ten behoeve van de operationele onderzoeken) opslaan van gegevens uit de voor interceptie gekozen communicatiedragers. Filteren is het proces dat bepalend is voor het verschil tussen de beschikbare gegevensstromen (communicatie) op de door de diensten gekozen communicatiedragers en de gegevens die uit die stromen uiteindelijk voor het inlichtingenproces worden opgeslagen.

Filteren is dus een reductieslag bij de verwerving van de ruwe communicatie (bulk) en moet daarom gezien worden als onderdeel van de verplichting tot datareductie. Het filterproces begint op het moment dat er een keuze wordt gemaakt voor een gegevensstroom, waarbij de voorafgaande keuze van de communicatiedrager wel kan bijdragen aan de gerichtheid van de interceptie maar geen deel uitmaakt van het filterproces. Het proces eindigt zodra gegevens worden opgeslagen ten behoeve van het verdere inlichtingenproces.

Bovenstaande definitie heeft tot gevolg dat de keuze om bijvoorbeeld een bepaalde satelliet (de drager) uit het totale aantal satellieten voor interceptie aan te wijzen geen filtering is. Filteren begint op het moment nadat de te intercepteren satelliet eenmaal is aangewezen en er een keuze gemaakt moet worden voor de op die satellietverbinding beschikbare communicatiestromen en eindigt wanneer gegevens ten behoeve van eventueel gebruik in het operationele proces in de databases van een van beide diensten worden opgeslagen. De verschillende keuzemomenten komen in de volgende paragraaf aan bod.

3.2 Filteren in het driefasenmodel

Gelet op de hiervoor gegeven definitie en omschrijving van het filterproces is duidelijk dat de toepassing van filters plaatsvindt in de eerste fase van driefasenmodel: de interceptie van de communicatie. Daarbij is het van belang aan te geven dat deze interceptiefase in de praktijk in drie onderdelen uiteenvalt, te weten a) de keuze van de te intercepteren communicatiedragers, b) de keuze en interceptie van de gegevensstromen en c) verdere filtering en opslag van de geïntercepteerde gegevens. Bij de uitvoering van deze onderdelen kunnen (uitkomsten van) processen uit de tweede en derde fase, in het bijzonder *search* gericht op interceptie, een rol spelen.

a) De keuze van de communicatiedragers

In de fase van verwerving gaat het allereerst om de keuze voor de communicatiedragers waarop de interceptiebevoegdheid wordt gericht.[19] Met betrekking tot interceptie van de kabel geldt dat dit plaatsvindt op een zogenaamde *access*-locatie, die aan de hand van het actuele dreigingsbeeld wordt gekozen. Op de *access*-locatie moeten de diensten een keuze maken uit de aanwezige (glasvezel)kabels (ook wel fibers genoemd). Ethercommunicatie laat zich onder meer onderscheiden in gegevensstromen via communicatiedragers als satellieten en (*high frequency*) radiogolven. De interceptie hiervan wordt

19 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 118.

gerealiseerd in Burum en Eibergen door het opvangen van de signalen met behulp van schotels en antennes.[20]

b) De keuze voor de gegevensstromen

Binnen de fibers van een kabel zijn vervolgens weer 'tientallen' kanalen te onderscheiden. In het geval van etherinterceptie van satellieten en (HF)radiogolven is sprake van gegevensstromen over uiteenlopende frequenties of frequentiebanden. Deze worden in het geval van satellietinterceptie linken genoemd. De diensten kiezen datastromen (en dus kanalen en linken) 'waarvan de gerede verwachting bestaat dat ze relevant zijn voor het beantwoorden van de onderzoeksopdrachten van de diensten'. [21]

De keuze voor bepaalde gegevensstromen komt allereerst voort uit kennis die bij de diensten aanwezig is, bijvoorbeeld in de vorm van bepaalde technische kenmerken (waaronder *leads*). Het zoeken naar de juiste kanalen of frequenties gebeurt bovendien aan de hand van *search* gericht op interceptie, wat tot doel heeft vast te stellen of inderdaad de informatie wordt onderschept die wordt beoogd. Daarbij nemen de diensten kennis van bijvoorbeeld protocollen, frequenties, taal maar ook de kwaliteit van de intercepties.[22] In het kader van *search* gericht op interceptie passen de diensten de praktijk van herhaaldelijk *snapshotten* (het kortstondig opnemen van inhoud en metadata) toe, wat inhoudt dat er wordt onderzocht of de kanalen of linken relevante communicatie bevatten. De keuze voor de concreet te intercepteren gegevensstromen kan dagelijks veranderen.[23] Dit maakt dat de keuze voor kanalen of linken (binnen respectievelijk fibers of satellieten) een vorm van filtering is.

Ten slotte vindt de daadwerkelijke interceptie van communicatie plaats door het signaal van de gewenste gegevensstromen (al dan niet eerst te kopiëren en) op te vangen. Daarbij is van tevoren (vaak) niet bekend wie via dat kanaal communiceert en is de kans groot dat ook communicatie wordt gekopieerd van personen en organisaties die geen onderwerp van onderzoek zijn en dat ook niet zullen worden.[24]

c) Verdere filtering en opslag van de geïntercepteerde gegevens

Niet alle opgevangen gegevensstromen worden ook opgeslagen ten behoeve van verdere verwerking. Tijdens en kort na de daadwerkelijke interceptie van gegevens vindt namelijk verdere filtering plaats. Voor een goed begrip is het van belang te onderscheiden tussen negatieve en positieve filters.[25] Een positief filter ziet doorgaans op de inhoud van communicatie, terwijl een negatief filter ziet op metadata.[26] Een negatief filter definieert gegevens die juist niet opgeslagen dienen te worden. Voorbeelden daarvan zijn datastromen van videodiensten als Netflix en YouTube. Gegevens die op basis van een negatief filter zijn uitgesloten, komen niet bij de diensten terecht, doordat ze worden 'afgebogen'.[27] Alle metadata die door dit filter heen zijn gekomen, worden opgeslagen.

Dat geldt ook voor inhoud die via positieve filtering is binnengekomen. Kort gezegd definieert een positief filter, bijvoorbeeld op basis van een bepaald technisch kenmerk (zoals een telefoonnummer), welke gegevens opgeslagen dienen te worden. De memorie stelt hierover: "In de praktijk wordt alleen inhoud opgeslagen wanneer duidelijk is dat die in fase 2 en 3 van het interceptieproces noodzakelijk is en binnen concrete onderzoeksopdrachten valt. Ten eerste op grond van locatiegegevens, specifieke versleuteling, landcodes bij telefonie, cyberkenmerken of een specifieke communicatietoepassing

20 CTIVD-rapport nr. 38 [5 februari 2014], p. 12.
21 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 110.
22 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 104.
23 CTIVD-rapport nr. 28 [23 augustus 2011], p. 28.
24 CTIVD-rapport nr. 38 [5 februari 2014], p. 12 e.v..
25 *Kamerstukken II 2016/17*, 34 588, nr. 18, p. 71 en 72.
26 *Kamerstukken II 2016/17*, 34 588, nr. 18, p. 18.
27 *Kamerstukken II 2016/17*, 34 588, nr. 18, p. 18. (Deze uitspraak is gedaan in de context van kabelinterceptie)

(fase 2). Daarmee is niet gezegd dat de inhoud meteen zeer lang wordt bewaard. Afhankelijk van de omstandigheden kan het ook gaan om een week of enkele maanden. Daarnaast wordt inhoud opgeslagen op grond van het feit dat het aan selectiecriteria (fase 3) voldoet, zoals nummers."[28]

Er zijn ook samengestelde filters, waarmee 'op intelligente wijze' gefilterd kan worden, bijvoorbeeld: "Verwijder alle spraakverkeer afkomstig van een satelliet, behalve vanuit een bepaald gebied." [29] Gegevens die niet door de verschillende filters heen zijn gekomen, worden niet opgeslagen en zijn op een later tijdstip dan ook niet meer terug te halen.[30] In het algemeen kan worden gesteld dat 'door de combinatie van het bepalen van de specifieke datastroom, de negatieve en positieve filtering alsmede tot slot de selectie van gegevens wordt gewaarborgd dat geen sprake is van het op grote schaal inbreuk maken op de privacy van personen die zelf geen onderwerp van onderzoek zijn'.[31]

28 *Kamerstukken II 2016/17*, 34 588, nr. 3, p. 110. (Deze uitleg ziet op zowel kabel- als satellietinterceptie)
29 *Kamerstukken II 2016/17*, 34 588, nr. 3, p. 98.
30 Bijlage bij *Kamerstukken II 2017/18*, 34 588, nr. 69, p. 3.
31 *Kamerstukken II 2016/17*, 34 588, nr. E, p. 2.

B.4 Vereisten voor de toepassing van filters in het kader van OOG-interceptie

Hoewel het woord filter in de wetstekst van de Wiv 2017 niet wordt genoemd, bestaat er wel een verplichting tot filteren. Deze situatie deed zich namelijk ook al voor in de Wiv 2002, waarbij de CTIVD in rapport 38 concludeerde dat het toepassen van filters moet worden gezien als onderdeel van de bevoegdheid tot ongerichte interceptie, die destijds was neergelegd in artikelen 26 en 27 Wiv 2002.[32] Er is geen aanleiding van deze zienswijze af te wijken. Deze interpretatie vindt bovendien steun in de wetsgeschiedenis van de Wiv 2017, onder meer omdat daarin de verplichting tot datareductie en een 'zo gericht mogelijke' toepassing van bijzondere bevoegdheden wordt benadrukt. In dit hoofdstuk worden de vereisten geformuleerd die aan de filters dienen te worden gesteld, zoals deze voor de AIVD en de MIVD uit de Wiv 2017 (inclusief de wetsgeschiedenis) en jurisprudentie kunnen worden afgeleid.

4.1 Taakstelling en onderzoeksopdrachten

De taakstellingen van de AIVD en MIVD staan respectievelijk in artikel 8 en 10 Wiv 2017 beschreven. Zij voeren deze taken uit in het belang van de nationale veiligheid. Ter uitvoering van hun taak kunnen de diensten gebruikmaken van verschillende bevoegdheden. Daaronder vallen ook bijzondere bevoegdheden. Artikel 28 lid 1 Wiv 2017 specificeert dat de inzet van bijzondere bevoegdheden alleen ter uitvoering van de wettelijke inlichtingen- en veiligheidstaken is toegestaan. In het kader van de nationale veiligheid mogen de diensten voor een beperkt aantal taken bijzondere bevoegdheden inzetten, te weten de a- en d-taak van de AIVD en de a-, c- en e-taak van de MIVD.

Door te stellen dat het onderzoek van communicatie onderzoeksopdrachtgericht moet zijn, wordt nadrukkelijk een koppeling gelegd met de Geïntegreerde Aanwijzing inlichtingen- en veiligheidsdiensten (GA). De onderzoeksopdrachten van de diensten zijn gebaseerd op de GA. Daarnaast kan er sprake zijn van acute onderzoeksopdrachten, die eveneens op ministerieel niveau worden geaccordeerd.

OOG-interceptie zal dus altijd in het kader van vooraf geformuleerde en geaccordeerde onderzoeksopdrachten moeten plaatsvinden. Dit begrenst de inzet en is van invloed op het inrichten van de filters, omdat deze eraan bij kunnen dragen om deze begrenzing te realiseren.

Tussenconclusie/concrete eis: OOG-interceptie moet plaatsvinden binnen het kader van de wettelijke inlichtingen- en veiligheidstaken en de op ministerieel niveau goedgekeurde onderzoeksopdrachten van de diensten, die voortvloeien uit de Geïntegreerde Aanwijzing inlichtingen- en veiligheidsdiensten (GA).

4.2 Zo gericht mogelijk

Op grond van artikel 5 van de Beleidsregels Wiv 2017 dient de toepassing van bijzondere bevoegdheden zo gericht mogelijk plaats te vinden.[33] Deze eis is geïntroduceerd als extra waarborg bij de toepassing van bijzondere bevoegdheden naar aanleiding van het raadgevend referendum.[34]

32 CTIVD-rapport nr. 38 [5 februari 2014], p. 14.
33 Beleidsregels Wiv 2017.
34 *Kamerstukken II* 2017/18, 34588, nr. 70 (brief van 6 april 2018) en toelichting Beleidsregels Wiv 2017.

Naast de noodzakelijkheidstoets, proportionaliteitstoets en subsidiariteitstoets vormt het gerichtheidsvereiste aldus een vierde toets bij de uitoefening van de bevoegdheden uit de Wiv 2017.[35] Het gerichtheidsvereiste behelst dat de diensten het verwerven van niet strikt voor het onderzoek relevante gegevens tot een minimum beperken, gelet op de technische en operationele omstandigheden van de casus.[36]

Dit geldt zeker voor de bevoegdheid tot OOG-interceptie, nu daar in de wetsgeschiedenis over is opgemerkt: "Onderzoeksopdrachtgerichte interceptie wordt zo gericht mogelijk ingezet. De wet staat niet toe dat bewust ruimer data wordt verzameld met het oog op latere toepassing." En in een ander stuk: "Het uitgangspunt bij onderzoeksopdrachtgerichte interceptie is dat de diensten zo doelgericht en effectief als mogelijk te werk gaan, met zo min mogelijk inbreuken op de persoonlijke levenssfeer van burgers."[37]

Artikel 32 van de Wiv 2017 bepaalt dat de bevoegdheid tot OOG-interceptie pas mag worden ingezet na toestemming van de minister en een rechtmatigheidstoets van de TIB. Artikel 29 lid 2 Wiv 2017 stelt eisen aan het verzoek om toestemming, zoals een aanduiding van de in te zetten bevoegdheid, een omschrijving van het onderzoek en de reden voor de inzet van de bevoegdheid. In aanvulling op deze eisen is in artikel 5 van de Beleidsregels Wiv 2017 bepaald dat bij het verzoek om toestemming nadrukkelijk wordt aangegeven op welke wijze aan de eis van gerichte inzet van de desbetreffende bijzondere bevoegdheid invulling wordt gegeven. Uit de toestemmingsaanvraag dient dan ook te volgen op welke wijze het toepassen van filters, als onderdeel van de interceptiebevoegdheid, leidt tot een 'zo gericht mogelijke' inzet daarvan. Dit behoort dientengevolge ook te zijn vastgelegd in beleid en werkinstructies van de diensten.

In een verdere aanvulling op de eisen van artikel 29 Wiv 2017, vereist artikel 48 lid 3 van diezelfde wet dat een verzoek om toestemming tot de inzet van OOG-interceptie, voor zover van toepassing, de reden moet bevatten waarom de uitoefening van die bevoegdheid ook betrekking moet hebben op de inhoud (naast de metadata) van telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk. Een tweede vereiste is dat er een typering van de vormen van telecommunicatie of gegevensoverdracht wordt gegeven.

Tussenconclusie/concrete eis: De inzet en de toepassing van de bevoegdheid tot OOG-interceptie moet, naast noodzakelijk, proportioneel en subsidiair, ook 'zo gericht mogelijk' zijn. Uit de toestemmingsaanvraag aan de minister en de TIB, evenals uit vastgelegd beleid en werkinstructies, dient concreet te volgen op welke wijze het toepassen van filters leidt tot een zo gericht mogelijke inzet. Voor zover het verzoek strekt tot de interceptie van inhoud, moet het daarvoor een motivering bevatten. In alle gevallen moet daarnaast een typering van de te onderscheppen communicatie in het verzoek zijn opgenomen.

4.3 Datareductie

Filters worden in de wetsgeschiedenis bovendien gezien als de voornaamste manier om aan de vereisten van *datareductie* te kunnen voldoen.[38] Zo stelt de memorie van toelichting: "Met name het

35 Zie de toelichting bij artikel 5 van de Beleidsregels Wiv 2017.
36 Reactie TIB op wijzigingsvoorstel Wiv 2017, p. 2.
37 *Kamerstukken II 2016/17*, 34 588, nr. 18, p. 72 en *Kamerstukken II 2016/17*, 34 588, nr. 3, p. 95.
38 De wet bevat met artikel 27 lid 1 een algemene verplichting om via bijzondere bevoegdheden verkregen gegevens zo spoedig mogelijk op relevantie te onderzoeken. Hieruit kan met betrekking tot OOG-interceptie echter geen algemene verplichting tot filteren afgeleid worden, omdat deze bepaling in artikel 48 lid 5 niet van toepassing is verklaard op gegevens uit OOG-interceptie. Die mogen volgens datzelfde lid maximaal drie jaar worden bewaard. Bovendien vloeit eruit voort dat als vast komt te staan dat de gegevens niet langer relevant zijn voor het onderzoek of andere lopende onderzoeken, ze terstond vernietigd moeten worden.

toepassen van filters bij de interceptie leidt ertoe dat de bulk aan gegevens die wordt geïntercepteerd, wordt gereduceerd tot die gegevens die voor verder onderzoek relevant kunnen zijn." Op deze manier is 'het zo snel mogelijk en zo veel mogelijk reduceren van de data in de eerste fasen van de interceptie een belangrijk onderdeel van het interceptieproces en een vereiste in het wetsvoorstel'.[39]

Uit bovenstaande is af te leiden dat filteren moet worden gezien als onderdeel van de verplichting tot datareductie in het kader van de interceptiebevoegdheid. Het proces speelt een belangrijke rol bij het scheiden van (potentieel) relevante en niet-relevante gegevens. Dit vindt plaats door te bekijken of in de te intercepteren gegevensstroom kenmerken voorkomen die aan actuele onderzoeksopdrachten of onderzoeken kunnen worden gerelateerd. Dit gebeurt met name aan de hand van geografische kenmerken van het verkeer of de aanwezigheid van selectiecriteria (zie daarvoor onder 4.5.3).

Artikel 48 lid 5 Wiv 2017 bepaalt ten slotte dat gegevens waarvan is vastgesteld dat deze niet relevant zijn voor het onderzoek dan wel enig ander lopend onderzoek vallend onder de in paragraaf 4.1 genoemde taken, terstond worden vernietigd.

Tussenconclusie/concrete eis: Filters moeten de geïntercepteerde communicatie terugbrengen tot die gegevens die (in potentie) relevant zijn voor de lopende onderzoeken van de diensten. Niet-relevante gegevens moeten terstond worden vernietigd (datareductie).

4.4 Kabelinterceptie

In delen van de wetsgeschiedenis komt terug dat in het geval van onderzoeksopdrachtgerichte interceptie op de kabel voor het positieve filter toestemming van de minister en de TIB is vereist. Bovendien wordt gesteld dat gegevens positief worden gefilterd op basis van selectiecriteria, zoals nummers. [40] Dit is echter geen eis in de wet zelf en wekt daardoor verwarring op. Sterker nog, de wet maakt mandatering van het vaststellen van selectiecriteria mogelijk. Het vragen van toestemming aan de minister en rechtmatigheidstoetsing door de TIB voor individuele criteria in het positief filter liggen daarmee niet voor de hand. Wel mag worden aangenomen dat alleen criteria in het positief filter mogen zijn opgenomen die zijn te herleiden naar een goedgekeurde last voor selectie (artikel 50 lid 2 Wiv 2017) of een last voor search gericht op selectie (artikel 49 lid 2 Wiv 2017).[41]

Met betrekking tot kabelinterceptie zijn er tijdens de behandeling van de Wiv 2017 ook specifieke opmerkingen gemaakt over de reductie van het datavolume. Zo wordt door middel van het toepassen van filters in de eerste fase van het interceptietraject naar verwachting 95 tot 98 procent van de geïntercepteerde data uiteindelijk niet opgeslagen.[42] Daarnaast is door de minister van BZK en de minister van Defensie gesteld dat het de komende jaren 'vrijwel uitgesloten' is dat verkeer met oorsprong en bestemming in Nederland onderschept zal worden, behalve in het kader van *cyber defence*.[43] Deze toezeggingen zijn in feite alleen te realiseren door middel van filters, waardoor ze van belang zijn voor dit onderzoek.

Tussenconclusie/concrete eis: In het geval van kabelinterceptie geldt dat het positief filter, gericht op de opslag van inhoud, alleen mag bestaan uit criteria in het kader van een goedgekeurde last tot (search gericht op) selectie. Uit de toepassing van filtering moet bovendien blijken dat de diensten rekenschap geven van de verwachting dat 95 tot 98 procent van het volume van de geïntercepteerde

39 *Kamerstukken II 2016/17*, 34 588, nr. 18, p. 71.
40 *Kamerstukken II 2016/17*, 34 588, nr. 18, p. 18 en Bijlage bij *Kamerstukken II 2017/18*, 34 588, nr. 69, p. 3.
41 Niet uitgesloten is echter dat ook in het kader van search gericht op interceptie (artikel 49 lid 1) een (ruim gedefinieerd) positief filter wordt gebruikt. Dit betreffen dan uiteraard wel kortstondige opnames.
42 *Kamerstukken II 2016/17*, 34 588, nr. 3, p. 111.
43 *Kamerstukken II* 2017/18, 34 588, nr. G, p. 3.

data uiteindelijk niet wordt opgeslagen en het vrijwel uitgesloten is dat communicatie met oorsprong en bestemming in Nederland (binnenlands verkeer), behalve in het kader van cyber defence, zal worden onderschept.

4.5 Overige invloeden op het toepassen van de filters

4.5.1 Verschoningsgerechtigden

De wet bevat specifieke regels over de inzet van bijzondere bevoegdheden met betrekking tot journalisten en advocaten. Artikel 30 lid 2 bepaalt dat als een bijzondere bevoegdheid, zoals OOG-interceptie, specifiek gericht is op een journalist en dit kan leiden tot 'de verwerving van gegevens inzake de bron van de journalist', de rechtbank Den Haag daar toestemming voor dient te verlenen na een verzoek van de minister. Lid 3 bepaalt vervolgens dat als de inzet van een bijzondere bevoegdheid ingezet wordt op een advocaat en deze uitoefening 'kan leiden tot de verwerving van gegevens die betrekking hebben op de vertrouwelijke communicatie tussen een advocaat en diens cliënt', de rechtbank eveneens toestemming moet verlenen.

Verder is ook artikel 27 lid 2 Wiv 2017 van toepassing op OOG-interceptie en bevat dit de verplichting gegevens terstond te vernietigen als het (voorzienbaar) gaat om vertrouwelijke communicatie tussen een advocaat en diens cliënt. Een uitzondering daarop is de situatie dat de verdere verwerking van de gegevens noodzakelijk is voor het onderzoek in het kader waarvan de gegevens zijn verworven en de rechtbank Den Haag daartoe toestemming heeft verleend. In de memorie wordt dit artikel toegelicht door te stellen dat het ziet op de situatie dat de communicatie tussen advocaat en cliënt 'als bijvangst' wordt binnengehaald bij de inzet van een bijzondere bevoegdheid jegens een ander. De conclusie in de memorie is daarbij dat het onwenselijk is om dit soort gegevens op voorhand uit te sluiten.[44]

Bovenstaande heeft tot gevolg dat de filters zo moeten worden ingesteld dat, anders dan in het geval van bijvangst, geen gegevens worden verworven die betrekking hebben op vertrouwelijke communicatie tussen een advocaat en diens cliënt of inzake de bron van een journalist. Het zonder toestemming van de rechtbank Den Haag in het positief filter zetten van kenmerken van advocaten en journalisten, of andere selectiecriteria die onontkoombaar leiden tot het verwerven van hun communicatie, is niet toegestaan. Deze eis gaat niet zo ver dat bijvangst moet worden uitgesloten door middel van een negatief filter.

Tussenconclusie/concrete eis: De diensten moeten het positief filter zo instellen dat geen gegevens worden verworven inzake de bron van een journalist of die betrekking hebben op vertrouwelijke communicatie tussen een advocaat en diens cliënt, tenzij daarvoor toestemming is verkregen van de rechtbank Den Haag. Deze eis gaat niet zo ver dat (meta)data van advocaten en journalisten moet worden uitgesloten door middel van een negatief filter.

4.5.2 Bijzondere persoonsgegevens

Een andere bepaling die van invloed kan zijn op de toepassing van filters is artikel 19 lid 3, dat vastlegt dat de verwerking van gegevens met betrekking tot iemands godsdienst of levensovertuiging, ras, lidmaatschap van een vakvereniging, gezondheid en seksuele leven niet plaatsvindt. Het vierde lid van dit artikel vormt daarop weer een uitzondering door te stellen dat de verwerking van dit soort gegevens alleen is toegestaan in aanvulling op de verwerking van andere gegevens en voor zover dat voor het doel van de gegevensverwerking onvermijdelijk is. Het gebruik van 'onvermijdelijk' geeft hierbij aan dat er een zwaardere toets geldt dan bij de algemene noodzakelijkheidstoets uit artikel 18 lid 1 Wiv 2017.[45] Dit vereiste vormt samen met de voorwaarde dat de gegevens alleen in aanvulling op

44 *Kamerstukken II 2016/17*, 34 588, nr. 3, p. 42.
45 *Kamerstukken II 2016/17*, 34 588, nr. 3, p. 34.

de verwerking van andere gegevens verwerkt worden een 'dubbel slot'. In de wetsgeschiedenis wordt het voorbeeld aangehaald dat 'de godsdienstige of levensovertuiging van personen geregistreerd wordt in de gevallen dat antidemocratische, staatsgevaarlijke of antimilitaristische activiteiten worden ontplooid waarbij deze personen hun godsdienstige of levensovertuiging als motief aanvoeren voor hun activiteiten'.[46]

Hier kan aangesloten worden bij bovenstaande redenering uit de memorie met betrekking tot advocaten, waarbij het onwenselijk is verklaard bepaalde gegevens op voorhand van interceptie uit te sluiten. Er bestaat dus geen verplichting deze negatief uit te filteren. Het in een positief filter opnemen van criteria die onontkoombaar en voorzienbaar leiden tot het verwerven van bijzondere persoonsgegevens, zonder dat dit onvermijdelijk is, is niet toegestaan.

Tussenconclusie/concrete eis: Het in een positief filter opnemen van criteria die onontkoombaar of voorzienbaar leiden tot het verwerven van bijzondere persoonsgegevens (gegevens met betrekking tot iemands godsdienst of levensovertuiging, ras, lidmaatschap van een vakvereniging, gezondheid en seksuele leven) is niet toegestaan, tenzij dit in aanvulling op de verwerking van andere gegevens gebeurt en voor zover dit voor het doel van de gegevensverwerking onvermijdelijk is.

4.5.3 Selectiecriteria

Omdat selectiecriteria veelal bepalend zijn voor de instelling van de positieve filters, komt de bijbehorende regeling hier kort aan bod. Voor de bevoegdheid tot selectie is volgens artikel 50 lid 2 en artikel 32 lid 2 toestemming van de minister en de TIB vereist. De bevoegdheid voor het vaststellen van selectiecriteria in lid 3 van artikel 50 ligt in beginsel bij de minister, maar kan aan het hoofd van de betreffende dienst gemandateerd worden. Ook verdere mandatering naar ondergeschikte ambtenaren is mogelijk. Daarmee heeft de (gemandateerde) ambtenaar een belangrijke functie in het waarborgen van een juiste instelling van de (positieve) filters.

Daarnaast is het mogelijk dat de (positieve) filters worden aangepast in verband met het verlenen van technische ondersteuning, te weten het selecteren van gegevens ten behoeve van partnerdiensten.[47] Deze vorm van ondersteuning vindt in de Wiv 2017 zijn weerslag in artikel 89 lid 4. Daarin is de bevoegdheid tot het verlenen van technische en andere vormen van ondersteuning neergelegd, waaraan een schriftelijk verzoek van de desbetreffende buitenlandse dienst vooraf moet zijn gegaan. De verlening van ondersteuning vindt plaats in het kader van de belangen van die buitenlandse dienst, voor zover deze verenigbaar zijn met de belangen van de Nederlandse diensten en de goede taakuitvoering zich niet tegen de verlening van ondersteuning verzet. Ook mag de ondersteuning er niet toe leiden dat de buitenlandse dienst zelfstandig gegevens verzamelt in Nederland.

4.5.4 Informatie van aanbieders van communicatiediensten

Op basis van artikel 52 zijn de diensten bevoegd om aanbieders van communicatiediensten te benaderen met een verzoek om gegevens te verstrekken. Aan de hand daarvan kunnen ze het 'communicatielandschap' in kaart brengen.[48] Dit is vooral voor het kiezen van de *access*-locatie voor kabelinterceptie van belang. Het vereiste van 'zo gericht mogelijke' interceptie dient daarbij te worden betrokken. Deze kennis kan immers ook van invloed zijn op een rechtmatige instelling van de filters.

46 *Kamerstukken II 2016/17*, 34 588, nr. 18, p. 26.
47 CTIVD-rapport nr. 38 [5 februari 2014], p. 34 e.v..
48 *Kamerstukken II 2016/17*, 34 588, nr. 3, p. 97.

4.6 Interne controle en effectief toezicht

De zorgplicht van artikel 24 van de Wiv 2017 voor een rechtmatige gegevensverwerking is een essentiële waarborg voor zowel de gegevensbescherming als het toezicht daarop. De bevordering van de kwaliteit van de gegevensverwerking is een nieuw element ten opzichte van de oude Wiv 2002. Dit onderdeel is in de Wiv 2017 opgenomen omdat meer en meer sprake is van geautomatiseerde gegevensverwerking door de diensten. De zorgplicht schept bovendien ook waarborgen bij de beoogde techniekonafhankelijkheid van de wet. De zorgplicht vraagt nadrukkelijk meer van de AIVD en de MIVD dan het enkel invoeren van de verplichtingen die de wet hen oplegt bij onder meer de verzameling, analyse en het gebruik van gegevens.[49]

Concreet betekent de zorgplicht dat de beide diensten voortdurend controle hebben op de wijze waarop zij gegevens verwerken en dat zij er zorg voor dragen dat de gegevensverwerking in overeenstemming is en blijft met de daarvoor geldende wettelijke voorschriften (*compliance*). Voortdurend in controle zijn vereist ook dat de diensten een aantal instrumenten gebruikt dat hun (centraal) zicht geeft op de werking van processen en systemen van gegevensverwerking en hen daardoor in staat stelt risico's te signaleren en tijdig maatregelen te nemen. Zonder dergelijke instrumenten, zonder een heldere structuur voor de zorgplicht, is het niet goed mogelijk voldoende interne controle uit te oefenen op de gegevensverwerking en is effectief extern toezicht daarop niet aan de orde.

Met betrekking tot filters bepaalt de Big Brother Watch-uitspraak van het EHRM bovendien dat het van belang is dat er onafhankelijk toezicht is op de zoek- en selectiecriteria die gebruikt worden om onderschepte communicatie te filteren.[50] Deze uitspraak is thans voorgelegd aan de Grote Kamer van het EHRM, waardoor de daarin vervatte conclusies nog niet definitief zijn.

Tussenconclusie/concrete eis: De diensten hebben een zorgplicht om interne controle uit te oefenen op de werking van de filters en de rechtmatige toepassing daarvan, om daarmee ook effectief extern toezicht op het proces van filteren mogelijk te maken.

49 CTIVD-rapport nr. 59 [27 november 2018], p. 7.
50 EHRM 13 September 2018, nrs. 58170/13, 62322/14 en 24960/15, ECLI:2018:0913JUD005817013, r.o. 340 en 347.

Postbus 85556
2508 CG Den Haag

T 070 315 58 20 | **F** 070 381 71 68
E info@ctivd.nl | www.ctivd.nl