# De Wet op de inlichtingen- en veiligheidsdiensten 2017: een technologisch gedreven wet[1]

J.J. Oerlemans & M. Hagens

## 1. Inleiding

In de aanloop naar het raadgevend referendum van 21 maart 2018[2] over de Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017)[3] werden de uiteenlopende opvattingen over de reikwijdte van de bijzondere bevoegdheden van de Nederlandse inlichtingen- en veiligheidsdiensten, te weten de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), duidelijk. Hét twistpunt over de Wiv 2017 in het kader van het raadgevend referendum was het voorstel tot 'onderzoeksopdrachtgerichte interceptie'; in de volksmond ook wel 'sleepnet' genoemd. Een breed verspreid beeld hierover was: *"De AIVD leest alle e-mails mee"*, "*een hele wijk wordt straks afgetapt*" en *"de AIVD gaat straks aan internet verbonden pacemakers hacken"*

Deels zijn deze angstbeelden verklaarbaar vanwege de 'techniekonafhankelijke' insteek van de Wiv 2017. Hierdoor wordt met brede begrippen gewerkt en kan een enkele bevoegdheid op veel verschillende wijzen zijn uitwerking krijgen. Ook is de toelichting op de wet dikwijls abstract geformuleerd, mogelijk om de *modus operandi* van de diensten te beschermen. Door nadere bestudering van de tekst van de wet, de toelichting op de wet en de parlementaire behandeling kan echter een genuanceerder beeld worden verkregen van de achtergrond en grenzen aan de toepassing van de bevoegdheden die in de wet omschreven staan.

In dit artikel wordt - ingegeven door de veranderingen op het gebied van de Informatie en Communicatie Technologie (ICT) - uitleg gegeven over vier bevoegdheden in de Wiv 2017.[4] Het gaat daarbij om: (1) onderzoeksopdrachtgerichte interceptie (art. 48-50), (2) de hackbevoegdheid (art. 45), (3) het stelselmatig vergaren van gegevens omtrent personen uit open bronnen (art. 38) en (4) de informantenbevoegdheid (art. 39). Daarnaast besteedt deze bijdrage aandacht aan de nieuwe waarborgen in de Wiv 2017 met betrekking tot toezicht en de verwerking van gegevens. Het doel is

---

[1] Citeertitel: J.J. Oerlemans & M. Hagens, 'De Wet op de inlichtingen- en veiligheidsdiensten 2017: een technologisch gedreven wet', *Computerrecht* 2018, nr. 3, p. 130-141.

* Jan-Jaap Oerlemans is verbonden als onderzoeker aan het Centrum voor Recht en Technologie van de Universiteit Leiden. Mireille Hagens is onderzoeker bij het departement Rechtsgeleerdheid van de Universiteit Utrecht. Beiden zijn werkzaam als onderzoeker bij de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). Dit artikel is op persoonlijke titel geschreven.

[2] De uitslag van het raadgevend referendum is dat 49,44% tegen en 46,53% voor de Wiv 2017 heeft gestemd. Naar aanleiding van deze uitslag kondigde de ministers van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en Defensie in hun Kamerbrief van 6 april 2018 enkele wijzigingen aan (*Kamerstukken II* 2017/18, 34588 en 34270, nr. 70; *Kamerstukken I* 2017/18, 34588, G). De Wiv trad op 1 mei 2018 in werking. De genoemde wijzigingen zijn voor zover relevant in dit artikel meegenomen.

[3] *Stb.* 2017, 317.

[4] Zie ook voor een bespreking van de relevante technologieën en invloed daarvan op bevoegdheden bijvoorbeeld ook David Anderson, 'A Question of Trust. Report of the investigatory powers review', Independent Reviewer of Terrorism Legislation, juni 2015 (hierna: Anderson 2015), p. 49-69. Zie voor besprekingen van de Wiv 2017 vanuit een andere invalshoek, bijvoorbeeld: R.J.I. Dielemans, 'De Wiv 2002 en Wiv 2017 op enkele hoofdlijnen vergeleken', *Justitiële verkenningen* 2018, nr. 1, p. 68-84 en het rapport van Q. Eijkman, N. van Eijk & R. van Schaik, 'Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Service Act 2017?', Utrecht/Amsterdam 2018.

een verklaring te geven voor de gewijzigde bepalingen in de Wiv met betrekking tot deze bevoegdheden en te illustreren hoe ontwikkelingen in de ICT het werk van inlichtingen- en veiligheidsdiensten ingrijpend veranderen. Dit artikel richt zich uitsluitend op het regelgevend kader voor de Nederlandse inlichtingen- en veiligheidsdiensten.

# 2. Onderzoeksopdrachtgerichte interceptie

Onderzoeksopdrachtgerichte interceptie is een vorm van 'bulkinterceptie' op communicatieverkeer. Het communicatieverkeer wordt onderschept en nader geanalyseerd ten behoeve van de taakuitvoering van de AIVD en de MIVD. In de praktijk wordt dit proces van bulkinterceptie uitgevoerd door de gezamenlijke 'Joint Sigint and Cyber Unit' (JSCU) van de beide diensten. Het proces wordt ook wel *signals intelligence* (sigint) genoemd, omdat de inlichtingen- en veiligheidsdiensten relevante informatie trachten te halen uit communicatie die zich op de één of andere manier via signalen voortbeweegt.[5] Daarbij kan gedacht worden aan satellietverkeer, mobiele telefoonverkeer, radioverkeer, *machine-to-machine* communicatie en internetverkeer 'over de kabel'.

## 2.1 Achtergrond van de bijzondere bevoegdheid

Voorheen, dat wil zeggen al ten tijde van de Wiv 2002, hadden de diensten de bevoegdheid communicatieverkeer uit 'de ether' - zoals satellietverkeer, GSM-verkeer en radioverkeer - op grote schaal te onderscheppen en nader te analyseren. De grote verandering in de Wiv 2017 is dat de beide diensten nu ook communicatieverkeer op de kabelinfrastructuur (zoals land- en zeekabels) mogen onderscheppen en analyseren. De uitbreiding naar 'bulkinterceptie op de kabel' vindt zijn achtergrond in de wijzigingen binnen de ICT in de afgelopen 15 jaar. Deze wijzigingen leidden tot problemen voor de inlichtingen- en veiligheidsdiensten, omdat deze in mindere mate dan voorheen relevante informatie uit communicatieverkeer uit de ether kunnen halen.[6] De commissie Dessens[7] verwoordde dit probleem als volgt:

"*De explosieve groei van internationale (glasvezel) kabelnetwerken heeft ertoe geleid dat naar schatting circa 80 tot 90% van het internationale dataverkeer nu via vaste netwerkverbindingen verloopt. De huidige juridische mogelijkheden voor ongerichte interceptie door de diensten zijn daardoor gereduceerd tot 10% à 20% van het telecommunicatie- en internetverkeer. (…) Door het snel groeiende verkeersvolume en het afnemende aandeel hiervan 'op de satelliet' maar ook door de toename van WiFi-netwerken, nieuwe informatie-infrastructuren, transities van internetprotocollen en 'nomadisch communicatiegedrag' nemen de mogelijkheden voor ongerichte maar ook gerichte interceptie af, waardoor de diensten op termijn 'doof en blind' dreigen te worden*"[8]

[5] In dit artikel valt onder 'sigint' nadrukkelijk ook het vergaren van gegevens 'op de kabel', waarbij het voorheen, ten tijde van de Wiv 2002, in een Nederlandse context ging om het vergaren en nader verwerken van gegevens uit satelliet- en radiocommunicatie (zie CTIVD rapport nr. 28 (2011) over de inzet van Sigint door de MIVD).

[6] Zie uitgebreid *Kamerstukken II* 2016/17, 34588, nr. 3, p. 8-11 en 91-95.

[7] De commissie Dessens heeft in 2013 een evaluatie uitgevoerd naar de Wiv 2002. Het evaluatierapport van de commissie Dessens, 'Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen' is als bijlage bij *Kamerstukken II* 2013/14, 33820, nr. 1 beschikbaar (hierna: Dessens 2013).

[8] Dessens 2013, p. 77.

Op zichzelf vormen deze wijzigingen in het telecommunicatielandschap en de manier van communiceren het belangrijkste argument voor de introductie van de bijzondere bevoegdheid in de Wiv 2017 die bulkinterceptie op de kabel zal toelaten. Hierbij moeten de volgende drie doelen van onderzoeksopdrachtgerichte interceptie (die ook het nut van de bijzondere bevoegdheid laten zien) in het achterhoofd worden gehouden.

## 1. Het kennen van de ongekende dreiging

Een belangrijke taak van inlichtingen- en veiligheidsdiensten is informatie te vergaren over personen en organisaties die *potentieel* de nationale veiligheid bedreigen. Een belangrijke functie van de AIVD en de MIVD betreft het 'kennen van de ongekende dreiging'. De diensten beschikken vaak over weinig informatie en een gefragmenteerd beeld van targets. Targets zijn personen of organisaties waar de AIVD of MIVD onderzoek naar verricht. Bulkinterceptie kan bijdragen aan de zoektocht naar missende informatie over targets en het identificeren van potentiële targets. Dit gaat als volgt in zijn werk. De onderschepte communicatie op een bepaald toegangspunt wordt opgeslagen en nader geanalyseerd. Daarbij spelen de metadata uit de onderschepte communicatie een belangrijke rol. Met behulp van metadata-analyse van de onderschepte communicatie kunnen bijvoorbeeld nieuwe telefoon- en IP-nummers van personen ontdekt worden die onder de aandacht van de AIVD of de MIVD staan of die van belang zijn voor een onderzoek maar nog niet eerder waren onderkend. Dit wordt *target discovery* genoemd.[9] Tijdens militaire missies draagt dit proces bijvoorbeeld bij aan het identificeren en lokaliseren van vijandelijke eenheden.[10] Het nut van sigint voor inlichtingen- en veiligheidsdiensten is overigens eerder uitgezocht door de Engelsen. Anderson geeft in zijn evaluatierapport bijvoorbeeld aan dat het bijdraagt in ongeveer 55% van de Britse inlichtingenrapporten. Het zou in het bijzonder nuttig zijn voor het bovengenoemde proces van *target discovery*, waarbij onbekende targets kunnen worden geïdentificeerd.[11]

## 2. Cybersecurity

Met behulp van bulkinterceptie op de kabel kan ook verdacht internetverkeer worden onderzocht. Bedrijven en overheidsorganisaties zijn in Nederland steeds vaker het slachtoffer van digitale spionage.[12] Voor de AIVD en de MIVD is een belangrijke taak weggelegd deze vorm van spionage vroegtijdig te detecteren en waar mogelijk te voorkomen. Om dat mogelijk te maken wordt gezocht naar de kenmerken van ongewenste activiteiten (bijv. *signatures* van kwaadaardige software) en naar verkeer dat ongebruikelijke afwijkingen vertoont (anomaliedetectie).[13] Verdacht communicatieverkeer wordt vervolgens verder onderzocht, waarmee mogelijk de actor achter een aanval uiteindelijk kan worden geïdentificeerd. Deze activiteit wordt *computer network defence* genoemd.[14] De Britten achtten bulkinterceptie op de kabel de *'critical enabler for the cyber defence*

[9] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 8-11, p. 93.
[10] Zie *Kamerstukken II* 2016/17, 34588, nr. 3, p. 8-11, p. 101.
[11] Anderson 2015, p. 128-129. Critici maken echter terecht de kanttekening dat de bevindingen gebaseerd zijn op aangedragen rapporten en informatie door de Britse communicatie-inlichtingendienst zelf.
[12] Zie bijvoorbeeld het Nationaal Cybersecurity Beeld 2015, 2016 en 2017.
[13] Zie *Kamerstukken II* 2016/17, 34588, nr. 3, p. 105. Hier wordt verder beschreven dat een verdacht gegevensbestand uit de interceptie nader wordt onderzocht. Ook wordt met behulp van de inzet van *deep packet inspection*-apparatuur gegevensverkeer geanalyseerd.
[14] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 94. Zie in dit kader ook Dessens 2013, p. 87.

*of the UK, providing the vast majority of all reporting on cyber threats and the basis for counter activity'*.[15]

## 3. Het leggen van verbanden tussen targets achteraf

De AIVD en de MIVD moeten ook na een aanval of incident kunnen duiden wat er heeft plaatsgevonden. Onderzoeksopdrachtgerichte interceptie draagt hieraan bij, omdat met de analyse van opgeslagen communicatieverkeer - in het bijzonder metadata - verbanden tussen targets kunnen worden gelegd, die de diensten niet eerder konden leggen. Als voorbeeld wordt in de memorie van toelichting bij de Wiv 2017 de aanslag in Parijs in 2015 genoemd. Na de aanslag konden inlichtingen- en veiligheidsdiensten met behulp van de analyse van onderschepte verkeersgegevens snel verbanden leggen tussen aanslagplegers aan de hand van historische metadata tot ruim twee jaar oud.[16] Incidenten leveren nieuwe informatie op die op basis van historische metadata-analyse cruciale inzichten biedt.

Het is belangrijk te realiseren dat de gegevens die worden vergaard uit onderzoeksopdrachtgerichte interceptie (zowel op de kabel als uit de ether) in de praktijk met andere inlichtingen- en veiligheidsdiensten kunnen worden uitgewisseld (zowel geëvalueerd als ongeëvalueerd). De gegevens worden uitgewisseld om andere landen op de hoogte te brengen van dreigingen, maar ook om het gefragmenteerde beeld uit onderschepte communicatie te complementeren.[17] Andere landen, zoals het Verenigd Koninkrijk, Frankrijk, Zweden en Duitsland, kennen al langer de bevoegdheid tot bulkinterceptie van communicatie in de ether als op de kabel.[18] Uit onder andere CTIVD-rechtmatigheidsonderzoeken naar de *signals intelligence* activiteiten van de Nederlandse diensten, blijkt dat de AIVD en de MIVD in samenwerkingsverbanden gegevens uitwisselen met buitenlandse inlichtingen- en veiligheidsdiensten.[19] Nederland is deels afhankelijk van deze gegevens ter bescherming van zijn nationale veiligheid. Als deze gegevens niet meer tot de beschikking van de AIVD en de MIVD staan, dan is Nederland minder goed beschermd dan voorheen. Deze kans was vóór de Wiv 2017 denkbaar, omdat buitenlandse inlichtingen- en veiligheidsdiensten werken op basis van het '*quid pro quo*'-principe: voor wat, hoort wat.[20] Met andere woorden: voor het verkrijgen van gegevens uit bulkinterceptie op de kabel van buitenlandse diensten, moet Nederland ook zelf gegevens aanleveren. Dit vormt ook een belangrijke reden waarom de aanpassing van de bevoegdheid in Nederland noodzakelijk werd geacht.

De AIVD en de MIVD kunnen aldus hun inlichtingenpositie verbeteren door gebruik te maken van onderzoeksopdrachtgerichte interceptie op de kabel. Het vormt een aanvulling op hun huidige repertoire aan sigint middelen teneinde een meer volledig beeld omtrent targets te kunnen krijgen.

---

[15] Anderson 2015, p. 130.
[16] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 100.
[17] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 158.
[18] Zie ook *Kamerstukken II* 2016/17, 34588, nr. 3, p. 11.
[19] Zie bijvoorbeeld CTIVD rapport nr. 38 (2014) inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD; CTIVD rapport nr. 49 (2016) over de uitwisseling van ongeëvalueerde gegevens door de AIVD en de MIVD, CTIVD-rapport nr. 56 (2018) over de multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten. Alle rapporten zijn te raadplegen via www.ctivd.nl.
[20] Zie *Kamerstukken II* 2016/17, 34588, nr. 3, p. 93 en 158. Zie ook CTIVD rapport nr. 38 (2014), p. 84 en 86.

De naam ‘onderzoeksopdrachtgerichte interceptie’ voor de bevoegdheid vindt zijn achtergrond in de ‘Geïntegreerde Aanwijzing inlichtingen- en veiligheidsdiensten’. In deze aanwijzing staat waar de behoeftestellers van de AIVD en de MIVD, dat wil zeggen de ministeries van Binnenlandse Zaken en Koninkrijksrelaties, Defensie, Justitie en Veiligheid en Buitenlandse Zaken, behoefte aan hebben en in welke mate de AIVD en de MIVD hieraan prioriteit in hun taakuitvoering dienen te geven.[21]

De precieze behoeftestelling en prioriteitsstelling in de bijlage van de Geïntegreerde Aanwijzing is staatsgeheim. In de memorie van toelichting op de Wiv 2017 worden echter de volgende drie voorbeelden gegeven: (1) het bieden van inzicht in aanslagplanning in Europa vanuit het ISIS-leiderschap in Syrië, (2) het onderkennen van digitale aanvallen vanuit Rusland en (3) het bieden van inzicht in de activiteiten van militante groeperingen in Mali.[22] Deze drie voorbeelden illustreren goed enkele concrete uitwerkingen bij de toepassing van de bijzondere bevoegdheid voor een van de taakstellingen van de AIVD en de MIVD, namelijk het beschermen van de nationale veiligheid en democratische rechtsorde.[23] Het werk van de MIVD is daarbij meer gericht op de strijdkrachten van andere mogendheden en de ondersteuning van de eigen strijdkrachten in conflictgebieden.[24] Daarbij wordt gepoogd in te schatten waar zich bedreigingen van de nationale veiligheid voordoen. Bij concrete dreigingsinformatie wordt deze informatie doorgezet naar de relevante overheidsdiensten die daar vervolgens binnen hun bevoegdheden op kunnen handelen.[25] De realiteit is dat de diensten met deze berichten aanslagen op Nederlandse doelen voorkomen.[26] Ook tijdens militaire missies kan dreigingsinformatie bijdragen aan het identificeren en lokaliseren van vijandelijke eenheden. Daarmee worden bijvoorbeeld medewerkers van Defensie beschermd, alsmede de manschappen van andere NAVO-landen binnen een coalitie.[27]

Op basis van voorbeelden en uitlatingen van een oud-directeur van de MIVD in aanloop naar het referendum lijkt bulkinterceptie op de kabel zich in de nabije toekomst meer te richten op communicatieverkeer met een focus op het buitenland, zoals communicatie van targets uit het buitenland naar Nederland en de interceptie van communicatie in conflictgebieden (o.a. ter bescherming van defensiemedewerkers).[28] Een aanzienlijk deel van de taken van de beide diensten is ook op het buitenland gericht, zelfs als het gaat om contra-terrorisme. Dat is anders voor onderzoeksopdrachtgerichte interceptie ten behoeve van cybersecuritydoeleinden, hetgeen eerder op binnenlandse communicatie (maar buitenlandse dreigingen) betrekking heeft. Hier wijzen wij er op dat in het buitenland, zoals het Verenigd Koninkrijk, expliciet ervoor wordt gekozen de

[21] Art. 6 Wiv 2017. Zie uitgebreid ook de oratie van Abels, ‘Per undas adversas? Geheime diensten in de maalstroom van politiek en beleid’, Universiteit Leiden 2018. Abels levert in zijn oratie kritiek op de rol en systematiek van de Geïntegreerde Aanwijzing.
[22] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 16.
[23] Zie artikel 8 lid 1 sub a Wiv 2017 voor de AIVD.
[24] Artikel 10 lid 1 sub a Wiv 2017.
[25] Het moge bekend zijn dat inlichtingen- en veiligheidsdiensten zelf niet over geweldsbevoegdheden of arrestatiebevoegdheden beschikken.
[26] Zie ook ‘AIVD verijdelde vier aanslagen in zes jaar tijd', redactie *Trouw*, 10 januari 2018.
[27] Zie *Kamerstukken II* 2016/17, 34588, nr. 3, p. 8-11 en p. 101.
[28] Zie Pieter Bindt, ‘Nieuwe Wet op Inlichtingen en Veiligheidsdiensten biedt goede balans tussen taken, bevoegdheden en waarborgen’, *ThePostOnline,* 21 februari 2018; en *Kamerstukken II* 2016/17, 34588, nr. 18, p. 18.

bulkinterceptiebevoegdheid vooral '*foreign focused*' in te zetten.[29] Het wordt daar niet wenselijk geacht de optie open te laten de bevoegdheid ook op binnenlands communicatieverkeer toe te passen. In Nederland wordt geen onderscheid gemaakt tussen het onderscheppen van communicatieverkeer met een focus op binnenlandse of buitenlandse communicatie. Wel is in reactie op de uitslag van het referendum gezegd dat het vrijwel uitgesloten is dat OOG-interceptie op de kabel de komende jaren wordt ingezet voor onderzoek naar communicatie met oorsprong en bestemming in Nederland (met uitzondering van onderzoek in het kader van cybersecurity).[30]

In de aanloop naar het referendum stelden veel tegenstanders van de wet, zoals initiatiefnemers van het 'sleepnetreferendum' of de Piratenpartij in Amsterdam, dat de bevoegdheid kan worden ingezet om het communicatieverkeer van een 'hele wijk' af te tappen.[31] Deze toepassing is niet waarschijnlijk om twee redenen: (1) het is niet snel proportioneel en subsidiair en (2) het is technisch lastig uitvoerbaar.[32] Alvorens de bijzondere bevoegdheid mag worden toegepast moet de minister toestemming geven, waarna de Toetsingscommissie Inzet Bevoegdheden (TIB) deze toestemming bindend toetst op rechtmatigheid, (zie paragraaf 6). Zij wegen daarbij af of de inzet van de bevoegdheid, met de privacy-inmenging voor betrokkenen als gevolg daarvan, in verhouding staat tot het doel van deze inzet (proportionaliteit). Daarnaast is de inzet niet toegestaan als minder vergaande middelen ter beschikking staan (subsidiariteit). De wetgever heeft zelf in het nader verslag uitgesloten dat de bijzondere bevoegdheid wordt ingezet om een hele wijk af te luisteren, omdat dit de bovengenoemde proportionaliteitstoets niet zal doorstaan.[33] Het ligt binnen Nederland veel meer voor de hand andere middelen in te zetten, zoals het voeren van een gesprek met mensen in die wijk en daarna het gericht aftappen van targets.

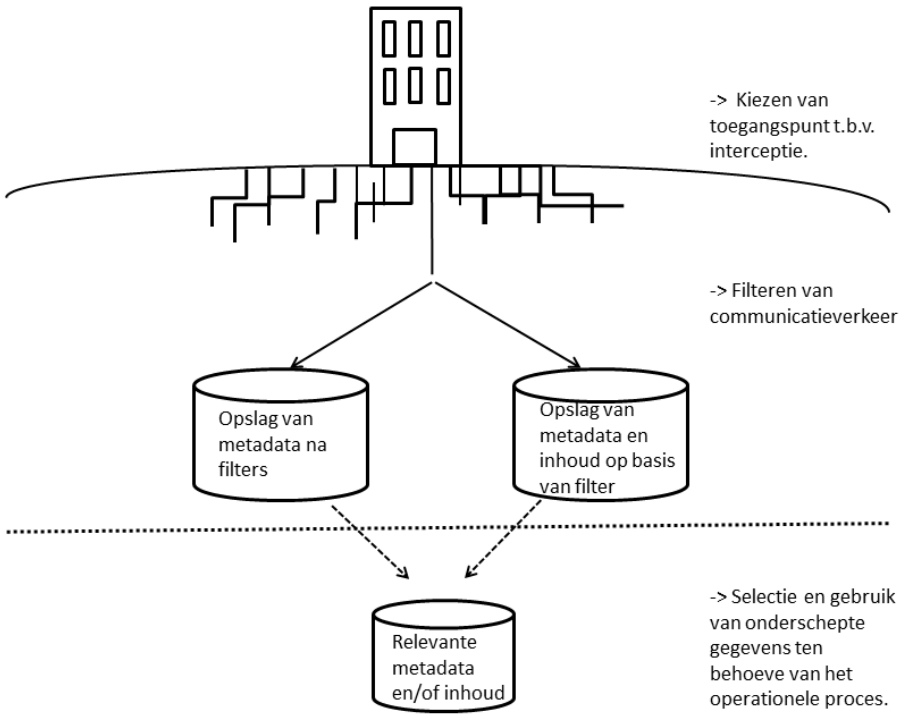
Daarnaast ligt het technisch gezien niet voor de hand alle communicatie uit een wijk af te tappen met behulp van bulkinterceptie op de kabel. Er is namelijk niet één toegangspunt voorhanden waar de diensten snel op kunnen 'inprikken' om vervolgens de relevante communicatie te onderscheppen en nader te analyseren.[34] Mensen maken daarvoor gebruik van te veel verschillende communicatiedienstverleners en toegangspunten. Om deze uitleg nog beter te begrijpen is het ook van belang het stelsel voor onderzoeksopdrachtgerichte interceptie kort te bespreken.

## 2.2 Stelsel van onderzoeksopdrachtgerichte interceptie

In deze paragraaf wordt kort een uitleg gegeven over het wettelijke stelsel van onderzoeksopdrachtgerichte interceptie om de reikwijdte van de bijzondere bevoegdheid meer duidelijk te maken. Hierbij ligt ten behoeve van dit artikel de nadruk op de kabel (het stelsel geldt immers ook voor interceptie van de ether). Het stelsel voor onderzoeksopdrachtgerichte interceptie op de kabel wordt hieronder in Figuur 1 geïllustreerd.

---

[29] Zie bijvoorbeeld de Britse factsheet over 'bulk interception', beschikbaar op: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473751/Factsheet-Bulk_Interception.pdf (laatst geraadpleegd op 13 maart 2018) en Anderson 2015, p. 79.
[30] *Kamerstukken I* 2017/18, 34588, G, p. 3.
[31] Zie bijvoorbeeld de website 'sleepwet.nl' en de video's op het YouTube-kanaal van de Piratenpartij in Amsterdam.
[32] Zie paragraaf 2.2.
[33] *Kamerstukken II* 2016/17, 34588, nr. 18, p. 9.
[34] Het uitvoeren van onderzoeksopdrachtgerichte interceptie op de kabel vergt veel voorbereidingstijd, waarbij de toegangspunten strategisch worden uitgekozen.




*Figuur 1: Vereenvoudigd model van onderzoeksopdrachtgerichte interceptie op de kabel.*

Aan de hand van Figuur 1 worden de belangrijkste aspecten van het interceptiestelsel aan de hand van de wet hieronder verder uitgelegd. Hierbij wijzen wij erop dat dit vereenvoudigde model gebaseerd is op de veronderstelde feitelijke uitoefening van onderzoeksopdrachtgerichte interceptie op de kabel en daaropvolgende verwerking van gegevens.[35] Het model in Figuur 1 komt niet één-op-één overeen met het 'drie-fasen model' uit de memorie van toelichting op de Wiv 2017.[36] Voor aansluiting met het fasen model hebben wij niet gekozen, omdat dat model doet voorkomen alsof de drie fasen van interceptie achtereenvolgend zijn, terwijl de bepalingen in de wet meer parallel aan elkaar lopen en met elkaar verweven zijn.[37]

### 2.2.1 Kiezen van toegangspunt en interceptie van de communicatie

De bevoegdheid communicatieverkeer te onderscheppen op een bepaald toegangspunt ('*access point*' genoemd) is geregeld in artikel 48 Wiv 2017. De betrokken internetdienstverlener, in de wet aanbieder van elektronische communicatiediensten of -netwerken genoemd, moet medewerking verlenen aan de uitoefening van de interceptiebevoegdheid.[38] Ten opzichte van de oude Wiv (2002) worden in de Wiv 2017 de categorieën van bedrijven die moeten meewerken aan de tenuitvoerlegging van de bijzondere bevoegdheid flink uitgebreid. Het betreft een uitbreiding van

[35] Vergelijk bijvoorbeeld het model van Koop (P.J.F. Koop, 'De Snowden-onthullingen en ongerichte interceptie onder de Wiv 2017', *Justitiële verkenningen* 2018, nr. 1, p. 133-147) en het model van onderzoeksopdrachtgerichte interceptie op de website van de AIVD, beschikbaar op: https://www.aivd.nl/onderwerpen/nieuwe-wet-op-de-inlichtingen--en-veiligheidsdiensten/onderzoeken-digitale-datastromen-oog-interceptie (laatst geraadpleegd op 20 maart 2018).
[36] Zie *Kamerstukken II* 2016/17, 34588, nr. 3, p. 90 t/m 124 en bijlage 4.
[37] De CTIVD heeft in haar Zienswijze op het wetsvoorstel voor de Wiv 2017 (november 2016) opgemerkt dat de fasen meer dan initieel werd gesuggereerd parallel aan elkaar lopen. Dit is in de memorie van toelichting erkend.
[38] Art. 51-53 Wiv 2017.

telecommunicatiebedrijven naar elektronische communicatiedienstaanbieders.[39] Dat betekent eenvoudig gesteld dat naast de telefoonaanbieder en internet access provider (voor toegang tot internet), óók hosting providers, cloud opslagaanbieders, besloten communicatieaanbieders en communicatiedienstaanbieders via apps (een voorbeeld van een zogenoemde 'OTT-diensten'), onder de medewerkersplicht van de Wiv 2017 vallen.[40] De medewerkingsverplichtingen kunnen uitsluitend worden afgedwongen jegens aanbieders die binnen de Nederlandse jurisdictie vallen.[41]

Voor de uitvoering van onderzoeksopdrachtgerichte interceptie zullen de AIVD en de MIVD in overleg treden met de aanbieders om na te gaan op welke plek in de infrastructuur van de aanbieder ze het beste het voor hun onderzoeksopdracht relevante communicatieverkeer kunnen onderscheppen. Ook houdt de medewerkersverplichting in dat aanbieders in overleg moeten treden over hoe de interceptie ten uitvoer kan worden gelegd.[42] Zelf aangebrachte versleuteling van de communicatie door de aanbieders moet ongedaan worden gemaakt, indien het betrokken bedrijf de kennis heeft de versleuteling ongedaan te maken.[43] In het nader verslag verduidelijkt de minister dat deze medewerkingsplicht niet inhoudt dat providers een 'achterdeur' in systemen moeten inbouwen teneinde toegang tot de ontsleutelde gegevens te krijgen. Ook is er geen enkele verplichting voor bijvoorbeeld aanbieders van communicatiediensten de encryptie die in hun systemen is toegepast te verzwakken'.[44]

De onderzoeksopdrachten in de Geïntegreerde Aanwijzing en 'acute onderzoeksopdrachten' vormen de basis voor de inzet van bulkinterceptie. Indien voldaan is aan de vereisten voor de inzet wordt zoveel mogelijk relevant communicatieverkeer onderschept. Ter uitvoering van de motie Recourt moet gedurende het gehele proces de bevoegdheid tegelijkertijd zo gericht mogelijk worden ingezet.[45] Ter uitvoering van de uitslag van het raadgevend referendum heeft de regering in april 2018 besloten dat deze verplichting in een beleidsregel wordt vastgelegd.[46] Communicatieverkeer loopt nu eenmaal niet via een vastomlijnd patroon. In de wet wordt daarom in artikel 49 Wiv 2017 voorzien in de mogelijkheid de communicatie constant te verkennen ter optimalisatie van de interceptie door steeds naar de relevante verkeersstromen te zoeken en de interceptie daarop aan te passen.[47]

---

[39] D. Verhulst, 'De Wiv 2017: sleepnet, aftapconsultancy en twijfelachtig toezicht', *Mediaforum* 2017, nr. 6, p. 182-186 (hierna: Verhulst 2017).
[40] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 84.
[41] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 241. Verhulst (2017, p. 184) stelt in haar artikel vragen bij deze rechtsmachtbepaling. In dat licht zijn ook de ontwikkelingen in België interessant, waarbij de Belgische justitie partijen als Yahoo! en Skype (zonder vestigingen in België) probeert te dwingen mee te werken aan de toepassing van bevoegdheden (zie ook Rb. van eerste aanleg Antwerpen, 27 oktober 2016, *Computerrecht* 2017/6, m.nt. E. Valgaeren).
[42] Zie artikel 52 en 53 Wiv 2017.
[43] Artikel 57 Wiv 2017.
[44] *Kamerstukken II* 2016/17, 34588, nr. 18, p. 66. Zie ook het aangenomen amendement van Verhoeven hierover (*Kamerstukken II* 2016/17, 34588, nr. 13).
[45] *Kamerstukken II* 2016/17, 34588, nr. 55. De aangenomen motie geldt overigens ook voor de andere bevoegdheden.
[46] *Kamerstukken II* 2017/18, 34588 en 34270, nr. 70; *Kamerstukken I* 2017/18, 34588, G.
[47] Zie *Kamerstukken II* 2016/17, 34588, nr. 3, p. 98. In de wet wordt dit overigens als een aparte fase ('fase 2') onderscheiden. De eerste fase vormt het kiezen van het toegangspunt en interceptie van de communicatie op dat punt.

### 2.2.2 Filteren van de relevante gegevens

Nadat het toegangspunt en de juiste datastroom is geselecteerd aan de hand van de onderzoeksopdracht wordt een enorme hoeveelheid netwerkverkeer onderschept. Niet-relevant verkeer moet terstond worden vernietigd. Mede daarvoor wordt een proces van filtering op het communicatieverkeer toegepast. In eerste instantie moet daarbij volgens de toelichting onder andere worden gedacht aan streamingdiensten, zoals Netflix-verkeer en YouTube-verkeer.[48] Videoverkeer over de kabel neemt een grote hoeveelheid volume van het totaalverkeer in beslag, zeker in aanmerking genomen dat steeds meer videoverkeer in hoge resolutie aan klanten wordt aangeboden. De AIVD en de MIVD geven aan dat als gevolg van deze datareductie uiteindelijk 98% van het onderschepte verkeer wordt vernietigd.[49] Alle metadata van het geïntercepteerde verkeer worden volgens de memorie van toelichting opgeslagen.[50]

Daarnaast wordt op basis van selectoren (zoals telefoonnummers, e-mailadressen en IP-adressen) bepaald – als zijnde een filter - welke communicatie wordt opgeslagen.[51] De selectoren zien op technische kenmerken van personen, organisaties en/of aan een nader omschreven onderwerp gerelateerde trefwoorden.[52] De verwachting is dus dat de analyse plaatsvindt op 2% van het totaal aan onderschepte netwerkverkeer. Niettemin wordt dan nog steeds een zeer grote hoeveelheid gegevens, waaronder veel metadata, opgeslagen door de AIVD en MIVD.[53]

Het opgeslagen communicatieverkeer na deze filtering mag voor analyse-doeleinden maximaal drie jaar worden opgeslagen.[54] Naar aanleiding van de uitslag van het raadgevend referendum is toegezegd dat elk jaar moet worden nagegaan of het noodzakelijk is de gegevens nog langer te bewaren.[55] De minister moet elk jaar toestemming geven de gegevens langer te bewaren (tot maximaal drie jaar). De ministers hebben toegezegd deze wijziging in een wijzigingswet te codificeren. De relatief lange maximale bewaartermijn van drie jaar wordt gemotiveerd met het argument dat ook lange tijd na bijvoorbeeld een aanslag, reeds opgeslagen (historische) metadata relevant kunnen zijn om 'terug te kijken'. Het kan enkele jaren duren om de relevantie van de gegevens vast te stellen, zoals ten behoeve van de identificatie van een nieuw target.[56]

### 2.2.3 Selectie en gebruik van gegevens voor operationele proces

De opgeslagen gegevens uit het communicatieverkeer worden vervolgens nader onderzocht. Op basis van artikel 50 Wiv 2017 kan dit gebeuren door middel van geautomatiseerde data-analyse,

---

[48] *Kamerstukken II* 2016/17, 34588, nr. 18, p. 71.
[49] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 111 en *Kamerstukken II* 2016/17, 34588, nr. 18, p. 76.
[50] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 110.
[51] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 106.
[52] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 108.
[53] De Directeur-Generaal van de AIVD, de heer Bertholee, sprak op 28 februari 2018 in het programma De Wereld Draait Door van een mogelijke doorloopsnelheid van 100 Gb per seconde op de kabel. Zelfs na een filtering tot 2% van het communicatieverkeer, wordt in dat geval een zeer grote hoeveelheid communicatieverkeer opgeslagen.
[54] De bewaartermijn van versleutelde gegevens kan telkens ter analyse met drie jaar langer worden verlengd (zie artikel 48 lid 6 Wiv 2017), omdat het lang kan duren voordat communicatie kan worden ontsleuteld (zie *Kamerstukken II* 2016/17, 34588, nr. 3, p. 102-103).
[55] Zie Kamerbrief van 6 april 2018 van de ministers van BZK en van Defensie (*Kamerstukken II* 2017/18, 34588 en 34270, nr. 70; *Kamerstukken I* 2017/18, 34588, G).
[56] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 108.

welke gericht is op het identificeren van personen of organisaties.[57] Daarbij moet gedacht worden aan het hierboven beschreven proces van het analyseren van metagegevens om tot nieuwe kenmerken en identificatie van targets te komen. Het opvragen van de opgeslagen gegevens met behulp van kenmerken van targets ter nadere analyse - al dan niet met software - wordt in de wet het proces van 'selectie' genoemd.[58] Daarbij kunnen de metadata ook worden gecorreleerd met andere gegevensbestanden die de diensten ter beschikking hebben.[59]

Voor de inzet van elk van de bevoegdheden in art. 48-50 Wiv 2017 is voorafgaand aan de daadwerkelijke inzet eerst toestemming van de minister van BZK of Defensie vereist en elke bevoegdheid moet afzonderlijk worden gemotiveerd. In de praktijk zal één keer toestemming worden gevraagd (een zogenaamde 'combinatielast') voor (1) het kiezen van het toegangspunt en het onderscheppen van de juiste communicatie samen met (2) het proces van selectie en geautomatiseerde data-analyse van de gegevens. Een combinatielast kan inzichtelijker maken hoe de drie bevoegdheden zich tot elkaar verhouden.[60] De toestemming van de minister voor een last wordt ook voorgelegd aan de nieuw ingestelde Toetsingscommissie Inzet Bevoegdheden (TIB) die dit bindend toetst (zie paragraaf 6). De verleende toestemming geldt voor een periode van drie maanden, respectievelijk een jaar.

Niet iedere medewerker van de AIVD en de MIVD heeft overigens toegang tot alle opgeslagen communicatieverkeer uit bulkinterceptie. In de toelichting wordt opgemerkt dat een (gecombineerd) stelsel van functie- en taakscheiding c.q. compartimentering wordt aangehouden, waarbij het gaat om de toegang van medewerkers van de AIVD en de MIVD tot de gegevens in de verschillende fasen in en buiten het interceptieproces.[61] Relevant bevonden gegevens voor het operationele proces worden vervolgens opgeslagen, totdat deze hun betekenis verliezen en dienen te worden verwijderd of bijvoorbeeld op basis van archiefwetgeving dienen te worden gearchiveerd.

## 3. De hackbevoegdheid

De Wiv 2002 kende reeds de bevoegdheid 'in geautomatiseerde werken binnen te dringen', oftewel computers te hacken.[62] Artikel 24 Wiv 2002 maakte het al mogelijk een technische voorziening op een computer te plaatsen, oftewel om software op een computer te plaatsen, versleuteling ongedaan te maken en daarmee bijvoorbeeld communicatieverkeer af te luisteren. Ten opzichte van de Wiv wordt in de Wet computercriminaliteit III voor een vergelijkbare hackbevoegdheid in het Wetboek van Strafvordering veel concreter uitgelegd dat met behulp van software communicatieverkeer 'op de bron' kan worden afgeluisterd, voordat het communicatieverkeer (zowel in schrift als audio) wordt versleuteld en daar een grote meerwaarde van de hackbevoegdheid zit.[63] Duidelijk is dat de hackbevoegdheid door de jaren heen voor de diensten belangrijker is geworden. In de memorie van toelichting op de Wiv 2017 wordt opgemerkt dat 'bij

[57] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 107. In de wet wordt dit als 'fase 3' van het interceptieproces beschreven.
[58] Zie artikel 50 lid 1 Wiv 2017.
[59] Zie ook *Kamerstukken II* 2016/17, 34588, nr. 3, p. 112.
[60] *Kamerstukken II* 2016/17, 34588, nr. 18, p. 75.
[61] Zie *Kamerstukken II* 2016/17, 34588, nr. 3, p. 96.
[62] In de memorie van toelichting wordt aangegeven dat de activiteiten tot uitvoering van de hackbevoegdheid ook wel '*computer network exploitation*' (CNE) wordt genoemd (*Kamerstukken II* 2016/17, 34588, nr. 3, p. 68).
[63] Zie *Kamerstukken II* 2015/16, 34372, nr. 3, p. 10.

targets van de diensten toegang tot de smartphone of tablet tegenwoordig vaak relevanter is dan bijvoorbeeld het binnentreden in een woning of het inzetten van een telefoontap'.[64]

Voorafgaand aan de inzet van de hackbevoegdheid in art. 45 Wiv 2017 moet de minister toestemming geven, dat vervolgens bindend door de nieuwe TIB op rechtmatigheid wordt getoetst. De CTIVD kan achteraf de rechtmatigheid van de toepassing van de bevoegdheid controleren (zie verder paragraaf 6.1 over toezicht).[65] In art. 45 lid 2 Wiv 2017 wordt de hackbevoegdheid gewijzigd ten opzichte van de Wiv 2002 door explicieter te maken dat met het plaatsen van software op computers daarmee ook andere opvolgende handelingen mogelijk zijn, zoals het observeren en afluisteren van een target via de computer.[66] De kenbaarheid en reikwijde van de hackbevoegdheid wordt door deze wijziging verbeterd.

Critici merken op dat de hackbevoegdheid nog steeds erg breed is geformuleerd. Het hacken van een smartphone van een target is immers van een andere orde dan het hacken van een provider, zo wordt gezegd.[67] Dat is inderdaad van een andere orde en hoewel de wet in potentie de bevoegdheid geeft de hackbevoegdheid op beide manieren in te zetten, moet de toepassing ervan uiteraard individueel gemotiveerd worden en getoetst worden aan de beginselen van noodzakelijkheid, proportionaliteit en subsidiariteit. Wel heeft de digitalisering van de samenleving de mogelijkheden en potentie van de hackbevoegdheid vergroot. Auteurs wijzen bijvoorbeeld ook op een wat extreme toepassing van de hackbevoegdheid waarbij mogelijk medische apparaten, zoals een pacemaker, worden gehackt.[68] Maar de mógelijkheid om een bevoegdheid in te zetten wil niet zeggen dat het ook daadwerkelijk wordt ingezet. In het nader verslag van de Wiv heeft de minister deze toepassing van de hackbevoegdheid zelfs al uitgesloten.[69] Ondanks de potentiële grote reikwijdte van te hacken apparaten zijn wij van mening dat er geen goede mogelijkheid bestaat de bevoegdheid tot hacken anders te formuleren, bijvoorbeeld door het te beperken tot bepaalde apparaten.[70] Inlichtingen- en veiligheidsdiensten moeten bovendien – binnen de kaders van de wet – een bepaalde vrijheid behouden op innovatieve wijze hun taak te kunnen uitoefenen en – met de benodigde controle daarop - een afweging te maken of een bepaalde inzet van de bevoegdheid te rechtvaardigen is.

---

[64] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 75.

[65] Zie in dat kader CTIVD-rapport nr. 53 over de inzet van de hackbevoegdheid door de AIVD en MIVD (2017).

[66] Zie artikel 45 Wiv 2017. Het artikel bevat overigens een - voor de Wiv - record van 12 leden.

[67] Zie bijvoorbeeld de reactie van J.V.J. van Hoboken en M.R. Koot op de internetconsultatie van de Wiv 2017, p. 5. Dat een hack op een provider niet geheel denkbeeldig is, laat een buitenlands voorbeeld zien waarbij wordt vermoed dat de Britse communicatie-inlichtingendienst de Belgische provider Belgacom heeft gehackt. Zie Huib Modderkolk, 'Waarom kwam de Britse geheime dienst zo makkelijk weg met het hacken van Belgacom?', *De Volkskrant*, 17 februari 2018.

[68] Zie bijvoorbeeld N.A.N.M. van Eijk & Q. Eijkman, 'Enkele kanttekeningen bij de Wiv 2017. De uitbreiding van bevoegdheden getoetst aan mensenrechten', *Justitiële verkenningen* 2018, nr. 1, p. 102 (hierna: Van Eijk & Eijkman 2018).

[69] *Kamerstukken II* 2016/17, 34588, nr. 18, p. 65: *"Ik kan mij echter nu en in de nabije toekomst geen enkele situatie voorstellen dat de diensten in het kader van het verzamelen van gegevens deze bevoegdheid zouden willen inzetten op een manier waarbij de lichamelijke integriteit van personen wordt aangetast. Ik sluit dat dus uit."*

[70] De auteurs hebben overigens zelf ook geen suggestie tot een andere wettekst met betrekking tot dit punt ingebracht. In de Wet computercriminaliteit III is de voorgestelde hackbevoegdheid in artikel 126nba Sv ook niet beperkt tot bepaalde apparaten. Daar is tijdens het parlementair debat wel bijvoorbeeld het hacken van een auto uitgesloten, omdat dit onaanvaardbare risico's voor andere weggebruikers met zich mee brengt (zie *Kamerstukken II* 2016/17, 34372, nr. 6, p. 32 en 53).

Een ander belangrijk kritiekpunt van de hackbevoegdheid betreft de mogelijkheid van de AIVD en de MIVD van kwetsbaarheden in hardware en software gebruik te maken ter uitvoering van de hackbevoegdheid.[71] Het argument is dat gebruikmaking van kwetsbaarheden computers en netwerken eigenlijk onveiliger maakt dan dat het veiligheid biedt. Dat geldt in het bijzonder voor onbekende kwetsbaarheden, omdat fabrikanten nog niet de mogelijkheid hebben gehad deze kwetsbaarheden met een 'patch' te dichten. Ook is het idee dat de diensten zodoende meewerken aan het in stand houden van een onethische markt van een handel in onbekende kwetsbaarheden, omdat onbekende kwetsbaarheden kunnen worden aangeschaft. Toch vindt de wetgever het wenselijk in bepaalde omstandigheden van onbekende kwetsbaarheden gebruik te kunnen maken ter bescherming van onze nationale veiligheid en democratische rechtsorde. De Nederlandse regering heeft een beleid ontwikkeld voor het gebruik van onbekende kwetsbaarheden in hardware en software ter uitvoering van de hackbevoegdheid. Dit beleid wordt in een unieke gezamenlijke brief van de ministers van Justitie en Veiligheid, Binnenlandse Zaken en Koninkrijksrelaties en Defensie uiteengezet.[72] In de brief staat dat de AIVD en de MIVD in principe de kwetsbaarheid moeten melden bij de fabrikant van hardware of software. Daarbij moet een afweging worden gemaakt met het belang van de bescherming van bronnen en operationele belangen, waardoor de melding kan worden uitgesteld. Als het zwaarwegend belang tijdelijk van aard is, dan zal de kwetsbaarheid daarna alsnog worden gemeld. Overigens blijkt in de praktijk dat slechts in 'enkele gevallen' bij toepassing van de hackbevoegdheid van onbekende kwetsbaarheden gebruik is gemaakt.[73]

Een laatste prominent kritiekpunt ziet op de mogelijkheid een *derde* te hacken met toepassing van de hackbevoegdheid.[74] De hack ziet daarmee niet op (een apparaat van) het target zelf, maar het apparaat van een ander ten behoeve van de uitoefening van de hackbevoegdheid op een target. Meer concreet wordt bedoeld dat het bijvoorbeeld mogelijk is een computer van een derde te hacken, omdat daar inloggegevens op staan die later kunnen worden gebruikt om een andere computer te hacken.[75] Het hacken van derden was ook al in de Wiv 2002 toegestaan, waarbij de CTIVD heeft aangetekend dat daarbij een verzwaarde subsidiariteitstoets moet plaatsvinden: het mag alleen als expliciet wordt gemotiveerd dat de toepassing onvermijdelijk is en er geen minder ingrijpende methoden voorhanden zijn om het doel te bereiken.[76] Deze bevoegdheid wordt in artikel 45 lid 5 Wiv 2017 expliciet in de wet vastgelegd, wat ten goede komt aan de kenbaarheid en reikwijdte van de bevoegdheid. Daar staat ook in dat de minister en TIB apart toestemming moeten geven voor het hacken van een derde. Daarbij is opgemerkt na een hack van een derde geen andere gegevens worden vergaard dan welke strikt noodzakelijk zijn voor het binnendringen van het

[71] Zie ook *Kamerstukken II* 2016/17, 34588, nr. 3, p. 305-306.
[72] Brief van 23 november 2016 (*Kamerstukken II* 2016/17, 26643, 428).
[73] Zie CTIVD-rapport nr. 53 (2017), p. 36. Zie bijvoorbeeld ook de bijdrage van de heer Prins aan de hoorzitting in de Tweede Kamer over de Wet computercriminaliteit III.
[74] Zie Koops e.a. 2016, 'Privacy Impact Assessment Wet op de inlichtingen- en veiligheidsdiensten 20XX', TILT/TNO, p. 104-105. De mogelijkheid de bevoegdheid op derden toe te passen is geregeld in art. 45 lid 5 Wiv 2017.
[75] Zie voor een vergelijkbaar voorbeeld bijlage II (toetsingskader) bij CTIVD-rapport nr. 53 (2017), p. 14.
[76] Zie uitgebreider: bijlage II (toetsingskader) bij CTIVD rapport nr. 53 (2017), p. 15; rapport zelf, p. 22.

geautomatiseerd werk van het target. De derde is immers niet meer dan een *'stepping stone'* om bij een computer van het target uit te komen.[77]

## 4. Stelselmatig vergaren van gegevens uit open bronnen

Vergeleken met de situatie in 2002 is veel meer informatie beschikbaar uit 'open bronnen' voor inlichtingen- en veiligheidsdiensten. In het bijzonder heeft de beschikbare informatie op internet en sociale media aan *'open source intelligence'* (OSINT) een nieuwe dynamiek gegeven. Ook de privacy-inmenging die potentieel plaatsvindt bij openbronnenonderzoek is in de afgelopen 15 jaar groter geworden, door de grotere hoeveelheid en aard van de persoonlijke gegevens op internet.[78] Bovendien kunnen deze gegevens met behulp van software, zoals *crawlers* en *scrapers*, worden vergaard en nader geanalyseerd.[79]

Het begrip open bronnen wordt in de Wiv 2017 gedefinieerd als bronnen die voor een ieder toegankelijk zijn, die 'zonder meer geraadpleegd kunnen worden en waarvoor geen drempels bestaan'.[80] Toch blijkt uit de memorie van toelichting op de Wiv 2017 dat ook informatie die commercieel voor een ieder beschikbaar is en informatie op sociale media, die na registratie voor een ieder beschikbaar is, als een open bron wordt beschouwd.[81]

De AIVD en de MIVD hebben een algemene bevoegdheid gegevens te verzamelen uit open bronnen. In art. 38 Wiv 2017 is ervoor gekozen openbronnenonderzoek te normeren als een bevoegdheid wanneer het op '*stelselmatige wijze'* plaatsvindt.[82] Aanleiding is waarschijnlijk de 'Privacy Impact Assessment' (PIA) van het wetsvoorstel voor de nieuwe Wiv geweest, waarin erop is gewezen dat ook openbronnenonderzoek tot een noemenswaardige inmenging met het recht op privacy leidt en daarom nader genormeerd moet worden.[83] Voor toepassing van de bevoegdheid in artikel 38 Wiv 2017 is toestemming van de betrokken minister of het hoofd van desbetreffende dienst vereist (met de mogelijkheid van ondermandaat). Ook moet een toets op proportionaliteit en subsidiariteit worden uitgevoerd. De auteurs van de PIA raadden aan er een *bijzondere* bevoegdheid van te maken, gezien de potentieel meer ernstige privacy-inmenging die zich hier kan voordoen.[84] Ook andere auteurs geven de voorkeur aan een regeling als bijzondere bevoegdheid.[85] De wetgever heeft hier niet voor gekozen, omdat het anders onder andere niet meer mogelijk zou zijn openbronnenonderzoek te doen tijdens bijvoorbeeld een veiligheidsonderzoek, omdat daarbij geen bijzondere bevoegdheden mogen worden ingezet.[86]

---

[77] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 79.
[78] Zie ook J.J. Oerlemans & B.J. Koops, 'Surveilleren en opsporen in een internetomgeving', *Justitiële verkenningen* 2012, vol. 38, nr. 5, p. 35-49.
[79] Zie verder A.R. Lodder & M.B. Schuilenburg, 'Politie-webcrawlers en Predictive policing', *Computerrecht* 2016/81, p. 150-154.
[80] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 38.
[81] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 55 en 63. Zie ook bijlage I bij CTIVD-rapport nr. 55 over het verwerven van door derden op internet aangeboden bulkdatasets (2018), p. 10-11.
[82] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 63 en *Kamerstukken II* 2016/17, 34588, nr. 18, p. 53.
[83] Zie Koops e.a. 2016.
[84] Koops e.a. 2016, p. 60.
[85] Zie de reactie van J.V.J. van Hoboken en M.R. Koot op de internetconsultatie van de Wiv 2017 en - in wat meer voorzichtige bewoordingen - Van Eijk & Eijkman 2018, p. 103-104.
[86] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 55.

Wij zijn ook van mening dat het doen van openbronnenonderzoek bij uitstek een bevoegdheid is die tot de algemene werkzaamheden van de diensten hoort en voor meerdere taken toepasbaar zou moeten zijn. Toch moet in de situatie waarbij grote hoeveelheden persoonsgegevens worden verwerkt met een technisch hulpmiddel (zoals software), worden nagedacht over het toepassen van aanvullende waarborgen met betrekking tot de gegevensverwerking en is mogelijk toestemming op een hoger niveau gewenst.[87] Niettemin vergroot het expliciet maken van de bevoegdheid de kenbaarheid en de reikwijdte van de bevoegdheden van de AIVD en de MIVD die zij ter beschikking hebben ter uitvoering van hun taakstelling.

Het is overigens curieus dat in de toelichting op de Wiv 2017 het criterium 'stelselmatig' niet nader wordt gedefinieerd. Naar verwachting wordt aangesloten bij het criterium van stelselmatigheid uit het strafrecht, waarvan sprake is als een 'min of meer volledig beeld van bepaalde aspecten van het privéleven' van de betrokkene wordt verkregen. Om dat te bepalen moeten factoren van de duur, frequentie, intensiteit en het gebruik van een technisch hulpmiddel in aanmerking worden genomen.[88]

## 5. De informantenbevoegdheid

Het opvragen van gegevens bij derden, in de Wiv 'informanten' genoemd, wordt door de wetgever gezien als een algemene bevoegdheid van de dienst.[89] Er gelden geen bijzondere toestemmingsvereisten, maar net als elke bevoegdheid kan een verzoek alleen met een bepaald doel worden gedaan en vindt er bij de toepassing een proportionaliteitstoets en subsidiariteitstoets plaats. De informantenbevoegdheid wordt gezien als een onderdeel van de algemene taakuitvoering van de AIVD en de MIVD en niet als een bijzondere bevoegdheid. Wel is de aard en toepassing van de bevoegdheid door de jaren heen gewijzigd als een gevolg van de digitalisering die ook bedrijven en overheidsinstellingen heeft geraakt. Tegenwoordig zijn meer gegevens beschikbaar dan voorheen, die met meer geavanceerde methoden kunnen worden geanalyseerd.

In de kern is de informantenregeling in de Wiv 2017 ongewijzigd ten opzichte van die van de Wiv 2002.[90] In de tekst van artikel 39 Wiv 2017 is nu opgenomen dat ook '*on line* en *real time*' verbinding kan worden gelegd tussen de dienst en de verstrekkende instantie, waarbij zonder menselijke

[87] Zie in dit kader ook het CTIVD-rapport nr. 55 (2018) en het toetsingskader in bijlage I van het rapport.
[88] Zie *Kamerstukken II* 1996/97, 25403, nr. 3, p. 26-27.
[89] Zie *Kamerstukken II* 2016/17, 34588, nr. 3, p. 55. De informantenbevoegdheid in artikel 39 Wiv 2017 valt eigenlijk uiteen in twee bevoegdheden: 1. Het opvragen van informatie bij een persoon, instelling of bedrijf die gegevens op vrijwillige basis verstrekt (hierbij geldt een legitimatieplicht voor de dienstmedewerker) en 2. Het loskrijgen van informatie van een persoon door middel van interactie (al dan niet onder dekmantel). De informant onderscheidt zich van een 'agent' doordat een informant niet door de AIVD of de MIVD wordt 'gestuurd'. Informanten krijgen van de diensten geen instructie tot het verzamelen van gegevens.
[90] Het is hierbij opvallend dat de wetgever in dit geval niet aansluit bij het stelsel in het Wetboek van Strafvordering. Zie hierover ook D.A. Korteweg, 'Rupsje nooitgenoeg: hoe de datahonger van de geheime diensten de wet normeert', *Tijdschrift voor Internetrecht*, nr. 5/6 2016, p. 200-202. Naar aanleiding van het advies van de Commissie Mevis is in strafvordering juist gekozen voor een gesloten stelsel van verstrekking van gegevens op basis van vorderingen, omdat het niet wenselijk werd geacht dat de verantwoordelijken voor gegevensverwerkingen zelf de afweging maakten of ze de gegevens op vrijwillig basis aan opsporingsautoriteiten in een opsporingsonderzoek verstrekken. Zie het rapport van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij 2001, p. 49, e.v. Slechts het verkrijgen van gebruikers- en verkeersgegevens bij telecommunicatieaanbieders met een vordering is in de Wiv in detail geregeld (artikel 54 en 55 Wiv 2017).

tussenkomst de diensten de gegevens kunnen opvragen en op vrijwillige basis verstrekt krijgen.[91] Volgens de memorie van toelichting bij de Wiv 2017 liet de Wiv 2002 reeds alle opties met betrekking tot de verstrekking van de gegevens open en is deze mogelijkheid van 'rechtstreeks geautomatiseerde toegang' slechts ingevoerd vanuit het oogpunt van kenbaarheid en rechtszekerheid.[92] Verder wordt uitgelegd dat in de praktijk afspraken gemaakt worden met de persoon, bedrijf of instelling (meestal een bedrijf of overheidsinstantie) over de manier waarop de gegevens ter beschikking worden gesteld. Het is namelijk vanwege de taakuitvoering van de diensten van belang dat het voor de gegevensverstrekker niet zichtbaar is welke gegevens worden opgevraagd. In de memorie van toelichting worden alle bepalingen uit de Wet bescherming persoonsgegevens (Wbp) buiten toepassing verklaard.[93] Het zou bijvoorbeeld niet logisch en niet wenselijk zijn als de verantwoordelijke aantekening houdt over de gegevensverstrekking en de betrokkene informeert over de gegevensverstrekking aan de diensten om daarmee aan bepalingen uit de Wbp te voldoen.[94]

De gegevensset kan *real time* aan de diensten ter beschikking worden gesteld, waarna medewerkers van de AIVD of de MIVD zoekslagen op de bron van gegevens kunnen uitvoeren. De data-analyse op de gegevensset, zoals het doorzoeken op profielen of naar patronen al dan niet in combinatie met andere bestanden, vindt 'idealiter' bij de diensten zelf plaats.[95] In een gegevensset zitten mogelijk ook veel gegevens van mensen die in beginsel niet in de aandacht van een van de diensten staan. Toch kunnen deze gegevens op basis van de informantenbevoegdheid worden verkregen en verwerkt wanneer daartoe aanleiding is. In artikel 19 Wiv lid 5 2017 staat dat dit mag indien deze [gegevens] een 'logisch en onlosmakelijk onderdeel vormen van de door de diensten te verwerven of verworven gegevensbestanden'. Het is daarbij wel belangrijk op te merken dat de raadpleging van de gegevens van de derde plaatsvindt op een 'hit/no hit basis': slechts die gegevens worden geraadpleegd waarop de zoekslag ziet.[96]

Het schrikbeeld van verschillende auteurs wordt goed geïllustreerd door dit citaat uit een artikel over de Wiv 2017 in 'De Correspondent':

"*De diensten hebben vanaf mei een wettelijke basis om geautomatiseerde toegang te krijgen tot databases van derde partijen. Ook hier is geen toestemming van de minister voor nodig. Denk aan een rechtstreekse koppeling met databases van bedrijven en organisaties die gegevens verwerken over identificatie, reisgedrag en financiën. Een paar concrete (maar hypothetische) voorbeelden: overheidsdatabases zoals de Basisregistratie Personen (BRP) en het kentekenregister, betalingsverkeer van banken, data van de OV-chipkaart, gegevens over kentekenregistraties door camera's op snelwegen, en gsm-mastdata waaruit blijkt wie met wie heeft gebeld, wanneer, hoelang, en op welke locatie.*"

[91] Zie artikel lid 4 Wiv 2017.
[92] *Kamerstukken II* 2016/17, 34588, p. 57-58.
[93] *Kamerstukken II* 2016/17, 34588, p. 57. Koning is hier bijvoorbeeld kritisch over in haar noot bij de *Tele2 Sverige AB*-zaak (HvJ EU, 21 december 2016, C-203/15, C-698/15, ECLI:EU:C:2016:970, *EHRC* 2017/79, m.nt. M.E. Koning).
[94] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 57.
[95] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 58.
[96] Zie ook *Kamerstukken II* 2016/17, 34588, nr. 3, p. 58.

Het is niet openbaar tot welke bronnen van gegevens de AIVD en de MIVD *real time* toegang hebben en in hoeverre het hierboven geschetste beeld klopt. Gezien de hoeveelheid gegevens en verregaande mogelijkheden tot verwerking van gegevens, betogen verschillende auteurs dat ook de informantenbevoegdheid een bijzondere bevoegdheid zou moeten zijn vanwege de ernstige privacy-inmenging die potentieel plaatsvindt.[97] Net zoals bij het stelselmatig vergaren van gegevens van personen uit open bronnen heeft de wetgever daar niet voor gekozen, omdat het historisch wordt gezien als een algemene bevoegdheid van de diensten die noodzakelijk is voor de uitvoering van al hun taken. Bovendien wordt het wenselijk geacht deze bevoegdheid ook te kunnen inzetten voor andere taken van de diensten, zoals het uitvoeren van veiligheidsonderzoeken. Bijzondere bevoegdheden mogen alleen worden ingezet voor de veiligheidstaken en de inlichtingentaken. Uit de praktijk moet nog blijken welke gegevensverwerkingen precies plaatsvinden en welke waarborgen daar precies bij horen.[98] Het laatste woord over deze bevoegdheid is dus nog niet gezegd.

# 6. Nieuwe waarborgen in de wet

In paragraaf 2-5 zijn enkele verstrekkende bevoegdheden uit de Wiv 2017 geanalyseerd. Daar hoort een stevig stelsel van waarborgen en toezicht bij, zoals hierna wordt uitgelegd. In deze paragraaf worden de nieuwe Toetsingscommissie inzet bevoegdheden (TIB) en enkele belangrijke nieuwe waarborgen met betrekking tot de verwerking van gegevens toegelicht.

## 6.1 Toezicht

De Commissie Dessens gaf in 2013 bij de evaluatie van de Wiv 2002 al aan dat een verruiming van de bijzondere bevoegdheden op het gebied van bulk kabelinterceptie gepaard moesten gaan met een versterking van het systeem van toestemming, controle en toezicht.[99] Dat hierbij verschillende keuzes mogelijk waren blijkt uit het vervolg. Dessens opteerde voor een versterking van het al bestaande onafhankelijke toezicht op de rechtmatigheid van de activiteiten van de AIVD en de MIVD (tijdens en achteraf) door de CTIVD, door enerzijds de rechtmatigheidsoordelen van de toezichthouder een bindende status te geven en anderzijds een snellere en intensievere controle van de lastgevingen voor de inzet van bijzondere bevoegdheden. Hieraan gaf Dessens de voorkeur boven de introductie in een nieuwe Wiv van toestemmingsverlening door een rechter, zoals in de Wiv 2002 op grond van artikel 13 van de Grondwet alleen vereist was voor het openen van brieven en postpakketten, of van voorafgaande bindende toetsing van de toestemming van de minister door een nieuw op te richten onafhankelijk orgaan.[100]

De wetgever maakte in de Wiv 2017 een andere keuze. De Wiv 2002 voorzag al in een solide stelsel van controle en toezicht op het werk van de geheime diensten bestaande uit een samenstel van

[97] Van Eijk & Eijkman 2018 en de reactie op in internetconsultatie van J.V.J. van Hoboken en M.R. Koot.
[98] In rapport nr. 55 over bulkdatasets heeft de CTIVD aangekondigd onderzoek te doen naar de rechtmatigheid van de uitvoering van de informantenbevoegdheid.
[99] Dessens 2013, p. 77.
[100] *Idem*, p. 95-101.

ministeriële toestemming, onafhankelijk toezicht door de CTIVD, parlementaire en rechterlijke controle en onafhankelijke klachtbehandeling door de Nationale ombudsman.[101]

Dit stelsel is (grotendeels) voortgezet in de nieuwe Wiv, met dien verstande dat – als tegenwicht tegen de uitbreiding van de bevoegdheden van de diensten – op bepaalde punten een versterking is voorzien. In de Wiv 2017 neemt de CTIVD de klachtbehandeling over van de Nationale Ombudsman ten aanzien van de AIVD en de MIVD en geeft daarbij een bindend oordeel. Dit gebeurt door de (nieuwe) afdeling klachtbehandeling. Een andere afdeling van de CTIVD (afdeling toezicht) oefent (gedurende en achteraf) toezicht uit op de rechtmatigheid van de activiteiten van de diensten.

Verder moet de rechtbank Den Haag toestemming geven voor de inzet van bijzondere bevoegdheden waar het de inzet tegen advocaten (vertrouwelijke communicatie) en journalisten (bronbescherming) betreft.[102] Dat mag slechts wanneer er sprake is van zwaarwegende operationele belangen, zoals het bestaan van een of meerdere aanwijzingen van een direct gevaar voor de nationale veiligheid. Deze toestemming geldt slechts voor vier weken in plaats van de gebruikelijke drie maanden. Een kritiekpunt is dat deze waarborg voor journalisten slechts geldt voor zover een bijzondere bevoegdheid wordt ingezet jegens een journalist en 'kan leiden tot de verwerving van gegevens inzake de bron van een journalist' (de 'directe inzet'). Deze bescherming is niet van toepassing als een bron een target is van de AIVD of de MIVD en met een journalist communiceert (de 'indirecte inzet').[103] Hierover werd tijdens de behandeling in de Eerste Kamer opgemerkt dat het te beschermen rechtsgoed in het geval van journalisten wezenlijk verschilt van dat van advocaten. Bij de laatste gaat het om de bescherming van de communicatie als zodanig tussen een advocaat en zijn cliënt in verband met het recht op een eerlijk proces. Dat maakt dat deze bescherming ook geldt als de verdachte zelf target van de dienst is en jegens hem bijzondere bevoegdheden worden ingezet. Bij journalisten gaat het volgens de regering om de bescherming van het recht dat zijn bronnen niet worden achterhaald. Er bestaat geen bijzondere bescherming voor een target om in vertrouwen met een journalist te kunnen communiceren.[104] Bovendien is de bescherming van het recht van journalisten op bronbescherming in het wetgevingstraject uitgebreid van het oorspronkelijke vereiste dat 'de inzet van bijzondere bevoegdheden moest zijn gericht op het achterhalen van een bron', naar de formulering dat 'de uitoefening van bijzondere bevoegdheden kan leiden tot de verwerving van gegevens inzake de bron van de journalist'.[105]

Een belangrijke noviteit is de instelling van de TIB die tot doel heeft de toestemming van de minister voor de inzet van bepaalde bijzondere bevoegdheden bindend op rechtmatigheid te toetsen voordat de inzet daadwerkelijk plaats heeft.[106] Dit geldt niet voor alle bijzondere bevoegdheden, wel voor gerichte en onderzoeksopdrachtgerichte interceptie, observatie, doorzoeken woning, DNA-

[101] Voor een bespreking van het toezichtstelsel in de Wiv 2002 zie M. Hagens, 'Toezicht op de Inlichtingen- en veiligheidsdiensten: een blik op het heden, het verleden en de toekomst', in: *Terrorisme. Studies over terrorisme en terrorismebestrijding*, E. Bakker e.a. (red.), Wolters Kluwer 2017, p. 555-594.
[102] Artikel 30 Wiv 2017.
[103] Het College voor de Rechten van de Mens en de Nederlandse Vereniging voor Journalisten hebben hierover kritiek geuit. De CTIVD pleitte in rapport nr. 52 over de inzet van bijzondere bevoegdheden jegens advocaten en journalisten door de AIVD en de MIVD ook voor eenzelfde beschermingsregime als voor de directe inzet.
[104] *Kamerstukken I* 2016/17, 34588, C (MvA), p. 32.
[105] *Kamerstukken I* 2016/17, 34588, C, p. 30-31.
[106] Zie *Kamerstukken II* 2016/17, 34588, nr. 3, p. 50-55.

onderzoek, hacken en informatie of medewerking vragen aan telecomproviders (art. 32 jo. 36 Wiv 2017). De TIB is geregeld in de artikelen 32 t/m 37 Wiv 2017.

De aanleiding voor de instelling van de TIB is te herleiden tot de vereisten die het Europees Hof voor de Rechten van de Mens en de Fundamentele Vrijheden (EHRM) in zijn jurisprudentie stelt aan geheim onderzoek van inlichtingen- en veiligheidsdiensten. Een belangrijke waarborg tegen misbruik en willekeur ziet het EHRM in voorafgaande onafhankelijke toestemming (of toetsing) voor de inzet van bijzondere bevoegdheden. Het EHRM heeft hierbij een sterke voorkeur voor de rechter, omdat hij het toonbeeld is van onafhankelijkheid en onpartijdigheid en bindende oordelen geeft. Dit laat onverlet dat de jurisprudentie ook ruimte biedt aan andere onafhankelijke instanties, mits zij beschikken over voldoende onderzoeksbevoegdheden en bindende oordelen kunnen geven.[107] Uit de jurisprudentie van het EHRM kan aldus worden afgeleid dat het systeem van waarborgen en toezicht op de inlichtingen- en veiligheidsdiensten geheel in balans dient te zijn, wat betekent dat de waarborg van voorafgaande onafhankelijke toestemming of toetsing geen wet van meden en perzen is als elders in het systeem wordt voorzien in onafhankelijk, bindend en effectief (rechterlijk) toezicht.[108] Toch heeft de wetgever in de Wiv 2017 wel de keuze gemaakt voor deze waarborg met de instelling van de TIB.

De instelling van de TIB is niet zonder kritiek gebleven. De TIB zou de toets van het EHRM niet kunnen doorstaan omdat het geen rechtelijk college is, onvoldoende onderzoeksbevoegdheden heeft en een serieus risico in zich draagt te verworden tot een stempelmachine.[109] Dessens wees al op deze risico's en benadrukte het belang te zorgen voor voldoende bevoegdheden, een goede benoemingsprocedure, informatievoorziening en een adequate ondersteuning. Ook is de effectiviteit van de instantie gebaat bij een wettelijke regeling die specifiek en vrij gedetailleerd aangeeft in welke situaties en onder welke voorwaarden een bevoegdheid mag worden ingezet, zodat de instantie beschikt over een duidelijk toetsingskader. Het gezag van de instantie en het publieke vertrouwen daarin kan vergroot worden door zo veel mogelijk openheid te geven over de werkzaamheden.[110]

De TIB is geen rechterlijk college in de zin van de Wet op de rechtelijke organisatie. Wel schrijft de Wiv 2017 voor dat ten minste twee van de drie leden, onder wie de voorzitter, ten minste zes jaar ervaring hebben als rechter (art. 33 lid 2 Wiv 2017). Als eerste lichting van de TIB zijn, op voordracht van de Tweede Kamer, bij koninklijk besluit benoemd Moussault (voorzitter), Mooy (lid) en Prins (ICT-expert) (art. 33). Hierbij past de overweging dat toestemming door de rechter verschillende beperkingen kent, waarbij, met name van belang is erop te wijzen dat het niet waarschijnlijk is dat een Nederlandse rechter zich zonder meer bevoegd zou achten om toestemming te verlenen voor de inzet van een bijzondere bevoegdheid in het buitenland. Aangezien een aanzienlijk deel van de activiteiten van de diensten betrekking heeft op het buitenland, is dit een realiteit die wordt

[107] EHRM (GC) 4 december 2015, *Roman Zakharov t. Rusland,* nr. 47143/06, *EHRC* 2016/87, m.nt. M. Hagens, par. 249/257-258; M. Hagens, 'Toezicht in de Wiv 2017. Kansen en uitdagingen voor een effectief en sterk toezichtstelsel', *Justitiële verkenningen* 2018, nr. 1, p. 85-98 (hierna: Hagens 2018).
[108] EHRM 12 jan 2016, *Szabo en Vissy t. Hongarije*, nr. 37138/14, par. 77.
[109] Zie bijvoorbeeld Van Eijk & Eijkman 2018, p. 105. Voor een bespreking van kansen en uitdagingen van toezicht in de Wiv 2017 zie nader Hagens 2018, p. 85-98 en Van Eijk & Eijkman 2018, p. 105-108.
[110] Dessens 2013, p. 96.

ondervangen met de TIB. Bovendien is de keuze voor een ICT-expert met praktijkervaring volgens ons een welkome aanvulling op de juridische expertise van de TIB, mede gezien de digitalisering van bevoegdheden die in dit artikel centraal staat.

De Wiv 2017 bepaalt dat de TIB haar toetsing uitvoert op basis van de toestemming van de minister (zijn besluit) en het daaraan ten grondslag liggende verzoek van de dienst (art. 36). De wet regelt verder dat de betrokken minister en dienst de TIB desgevraagd alle inlichtingen moeten verstrekken en alle medewerking moeten verlenen die de TIB voor haar goede taakuitoefening noodzakelijk acht. De TIB beoordeelt of de inzet van een bijzondere bevoegdheid 'rechtmatig' is, dat wil zeggen noodzakelijk is voor een goede taakuitvoering van dienst, in een redelijke verhouding staat tot het doel (proportionaliteit), het minst ingrijpende middel is, (subsidiariteit) en zo gericht mogelijk wordt toegepast.

De toetsing door de TIB wordt in het stelsel aangevuld met het rechtmatigheidstoezicht van de afdeling toezicht van de CTIVD. Hoewel niet in de wet vastgelegd, hebben beide instanties volgens de ministers expliciet als taak om waar nodig afstemming te zoeken en de rechtseenheid te bewaken.[111] Kenmerkend voor het toezicht van de CTIVD is dat het meer de breedte en de diepte ingaat dan de toetsing vooraf. Voor wat betreft het toezicht op de bulk kabelinterceptie heeft de CTIVD in zijn 'Eindbalans' over de Wiv 2017 aangegeven dat er voldoende mogelijkheden zijn voor effectief toezicht op zowel de werking van het systeem als op de toepassing en uitwerking daarvan in concrete gevallen.[112]

## 6.2 Zorgplicht en de verwerking van gegevens

De Wiv 2017 bevat enkele nieuwe waarborgen op het gebied van gegevensverwerking. De in de Wiv 2017 geïntroduceerde *zorgplicht* voor de kwaliteit van de gegevensverwerking is daarbij van bijzonder belang. Deze zorgplicht houdt in dat de hoofden van de diensten zorgdrager zijn voor de technische, personele en organisatorische maatregelen ter bevordering van de kwaliteit van de gegevensverwerking.[113]

Deze zorgplicht biedt de CTIVD de mogelijkheid de kwaliteit van de verwerking van gegevens te toetsen, maar bijvoorbeeld ook de processen die de kwaliteit van gegevensverwerking moet waarborgen.[114] Daaronder vallen ook modellen en algoritmen die mogelijk worden gebruikt voor bijvoorbeeld metadata-analyse op de onderschepte gegevens.[115] Hierover moeten de diensten verantwoording afleggen (compliance). De toezichthouder investeert, onder meer voor de controle op de uitvoering van deze zorgplicht door de diensten, in de nodige (technische) expertise.

De Wiv 2017 bevat ook strengere regels over het bewaren van gegevens. Nieuw is de invoering van een 'relevantietoets' bij de verwerving van gegevens uit bijzondere bevoegdheden. Dit betekent dat zo snel mogelijk een onderzoeksplicht op relevantie moet plaatsvinden binnen een jaar dat de gegevens zijn verkregen door toepassing van een bijzondere bevoegdheid, zoals de

[111] *Kamerstukken I* 2016/17, 34588, nr. C (MvA), p. 20.
[112] CTIVD Eindbalans Wiv 2017, p. 5.
[113] Zie artikel 24 Wiv 2017.
[114] Zie ook CTIVD Eindbalans Wiv 2017.
[115] Zie artikel 24 lid 2 sub a Wiv 2017. *Kamerstukken II* 2016/17, 34588, nr. 18, p. 8.

hackbevoegdheid of gerichte tapbevoegdheid.[116] Slechts gegevens die relevant zijn voor het onderzoek of enig ander onderzoek mogen worden bewaard; de rest moet terstond vernietigd worden.[117] Alle gegevens die door de AIVD en de MIVD verwerkt worden moeten op grond van artikel 20 Wiv 2017 verwijderd worden als deze niet meer van betekenis zijn.

# 7. Conclusie

Digitalisering heeft invloed op de toepassing en reikwijdte van de bevoegdheden die zijn toebedeeld aan de AIVD en de MIVD. Dit komt met betrekking tot de bevoegdheden in de Wiv 2017 op verschillende wijzen tot uiting. Onderzoeksopdrachtgerichte interceptie wordt bijvoorbeeld uitgebreid naar interceptie 'op de kabel' met meer medewerkingsverplichtingen voor communicatieaanbieders. Op deze manier kan bijvoorbeeld meer internetverkeer worden onderschept en nader worden geanalyseerd. Dat is volgens de diensten noodzakelijk, omdat steeds meer communicatie via internet verloopt. De hackbevoegdheid wordt volgens de wetgever ook steeds belangrijker om inlichtingen te vergaren. Verder is meer informatie dan voorheen publiekelijk beschikbaar op het internet en zijn er meer (grootschalige) datasets van overheidspartijen en particulieren voorhanden dan in 2002. Deze ontwikkelingen en wijzigingen in de Wiv 2017 zijn in dit artikel geanalyseerd en becommentarieerd. Hier tegenover staat een robuust stelsel van toezicht en waarborgen omtrent gegevensverwerking dat ook belangrijke veranderingen heeft ondergaan.

Uit de praktijk zal blijken hoe de AIVD en de MIVD omgaan met de gewijzigde bevoegdheden en nieuwe bepalingen uit de wet. Hierbij is van belang op te merken dat (onderdelen van) onderzoeksopdrachtgerichte interceptie al binnen twee jaar na de inwerkingtreding van de wet wordt geëvalueerd door de CTIVD. De ministers van BZK en van Defensie hebben daarnaast in Kamerbrieven een vervroegde evaluatie van de Wiv 2017 toegezegd door een apart in te stellen onafhankelijke commissie twee jaar na inwerkingtreding van de wet.[118] Ondertussen voert de CTIVD ook haar toezichtstaak uit door, onder andere, de uitoefening van bevoegdheden op rechtmatigheid te controleren en daarover via openbare rapporten te rapporteren. De nieuw ingestelde TIB zal de toepassing van vele bijzondere bevoegdheden vooraf controleren. Het is de verwachting dat hiermee meer duidelijkheid komt over de uitwerking van bepaalde wettelijke bepalingen en dat eventuele tekortkomingen hierin komen bovendrijven.

Niet uitgesloten is dat over een jaar of vijf alweer een nieuwe Wiv in voorbereiding wordt gesteld die inspeelt op maatschappelijke en politieke ontwikkelingen, waaronder de voortgaande digitalisering van de samenleving, en de daarbij horende rechtsbescherming. Digitalisering brengt nu eenmaal gevolgen met zich mee met betrekking tot de toepassing van bevoegdheden. Van tijd tot tijd moet wetgeving daarop worden aangepast om zowel de noodzakelijke instrumenten aan de inlichtingen- en veiligheidsdiensten te geven als te voorzien in adequate waarborgen en normering ter bescherming van de fundamentele rechten en vrijheden van burgers.

[116] Artikel 27 Wiv 2017. De termijn waarbinnen de relevantietoets plaatsvindt kan met toestemming van het hoofd van de desbetreffende dienst met zes maanden worden uitgesteld.
[117] Voor onderzoeksopdrachtgerichte interceptie geldt zoals in paragraaf 2.2.2 aangegeven een afwijkende bewaartermijn van drie jaar. Bovendien hoeven die gegevens niet 'terstond vernietigd' te worden.
[118] O.a. *Kamerstukken II* 2017/18, 34588, nr. 69, p. 3 (brief van minister van BZK, mede namens de minister van Defensie, van 19 december 2017 over de Wiv 2017 en het regeerakkoord).