Privacy en bulkinterceptie in de Wiv 2017

J.J. Oerlemans & M. Hagens[*]

De bevoegdheid tot het in bulk tappen van de kabel is nieuw in de Wet op de inlichtingen- en veiligheidsdiensten 2017 en heeft tot veel discussie geleid. In dit artikel bespreken de auteurs hoe het Nederlandse stelsel van 'onderzoeksopdrachtgerichte interceptie' (bulkinterceptie) en 'geautomatiseerde data-analyse' zich verhoudt tot het recht op privacy in de jurisprudentie van het EHRM.

1. Inleiding

Voor het themanummer 'Privacy' van Ars Aequi vroeg de redactie ons een artikel te schrijven over de 'Sleepwet'. De toon was gezet! Binnen de redactie heerst, net als bij veel andere Nederlanders, blijkbaar het beeld dat de uitbreiding van de bevoegdheden van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD) de nieuwe Wet op de inlichtingen- en veiligheidsdiensten 2017 (hierna: Wiv 2017[1]) tot een 'sleepwet' maakt. Deze framing is ontstaan tijdens de totstandkoming van de wet en in de aanloop naar het raadgevend referendum op 21 maart 2018 over de Wiv 2017.[2]

Rondom het raadgevend referendum over de Wiv 2017 ging de discussie vooral over de nieuwe bijzondere bevoegdheid van het in bulk tappen van communicatie ('bulkinterceptie'), in de Wiv 'onderzoeksopdrachtgerichte interceptie' genoemd. Deze bevoegdheid wordt in de volksmond ook wel 'sleepnet' genoemd. Dat op deze manier grote hoeveelheden gegevens van burgers kunnen worden verzameld en geanalyseerd is zeker waar. In het huidige digitale tijdperk zijn steeds meer gegevens beschikbaar. Deze veranderde context maakt dat ook met andere bevoegdheden van de AIVD en MIVD in de Wiv 2017 grote hoeveelheden gegevens kunnen worden verkregen en verwerkt. Het hoeft niet eens te gaan om een bijzondere bevoegdheid, zoals de hackbevoegdheid. Het vergaren van gegevens 'in bulk' is ook mogelijk met de inzet van de algemene bevoegdheden, zoals de informantenbevoegdheid.[3] Ook hiermee kan een ernstige inbreuk op de persoonlijke levenssfeer van personen worden gemaakt. Dat betekent nog niet dat de Wiv 2017 kwalificeert als een 'sleepwet'. Van belang is dat de wet en de uitvoering ervan in de praktijk een juiste balans treft tussen het belang van nationale veiligheid waarvoor deze bevoegdheden bestaan en de rechtsbescherming van de burger.

De totstandkoming van de wet en het referendum liggen inmiddels al enige tijd achter ons. De Wiv 2017 is per 1 mei 2018 in werking getreden. Sindsdien heeft het Europees Hof voor de Rechten van de Mens (EHRM) zich in de Britse en Zweedse zaken *Big Brother Watch e.a.* en *Centrum för Rättvisa* uitgesproken over bulkinterceptie en verdere verwerking (analyse) van communicatie in de context van nationale veiligheid en de daarvoor geldende waarborgen. In dat verband lijkt het ons goed nog

---

[*] Mr. dr. Jan-Jaap Oerlemans is verbonden als onderzoeker aan het Centrum voor Recht en Technologie van de Universiteit Leiden. Mr. dr. 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. Citeerwijze: J.J. Oerlemans & M. Hagens, 'Privacy en bulkinterceptie in de Wiv 2017', *AA* 2019/7, p. 560-568.

[1] *Stb.* 2017, 317.

[2] De uitslag van het raadgevend referendum is dat 49,44% tegen en 46,53% voor de Wiv 2017 heeft gestemd.

[3] Wij hebben deze (bulk)bevoegdheden beschreven en geanalyseerd in het kader van de Wiv 2017 en de daarbij geldende waarborgen in J.J. Oerlemans & M. Hagens, 'De wet op de inlichtingen- en veiligheidsdiensten 2017: Een technologisch gedreven wet', *Computerrecht* 2018/111, nr. 3, p. 130-141.

eens stil te staan bij het stelsel van onderzoeksopdrachtgerichte interceptie en geautomatiseerde data-analyse als onderdeel daarvan in de Wiv 2017. Vragen die hierbij aan de orde komen, zijn: hoe zijn deze bevoegdheden geregeld? Welke waarborgen zijn daarbij voorzien voor de rechtsbescherming van burgers? Hoe verhoudt zich dit tot de jurisprudentie van het EHRM? Of daarna het beeld van een 'sleepwet' overeind blijft, is uiteindelijk ter beoordeling van de lezer.

2. De betekenis van *Centrum för Rättvisa* en *Big Brother Watch e.a.* voor bulkinterceptie

Het EHRM heeft in 2018 uitgebreid de relatie besproken tussen 'bulkinterceptie' (dat is de benaming die het EHRM daaraan geeft), de analyse van metagegevens[4] van communicatie door inlichtingen- en veiligheidsdiensten en het recht op privacy in artikel 8 van het Europees Verdrag van de Rechten van de Mens en de Fundamentele vrijheden (EVRM) in twee arresten *Centrum för Rättvisa t. Zweden* en *Big Brother Watch e.a. t. Verenigd Koninkrijk*.[5] Deze arresten zijn uiteraard ook van belang voor Nederland, omdat hier algemene beginselen uit volgen en kwalitatieve vereisten waaraan nationale regelgeving moet voldoen die wij hierna toelichten.

Hierbij past de kanttekening dat de zaken *Big Brother Watch e.a.* en *Rättvisa* inmiddels zijn geaccepteerd voor behandeling door de Grote Kamer van het EHRM. Als gevolg daarvan krijgen de zaken een geheel nieuwe beoordeling. De mogelijkheid bestaat dat de Grote Kamer van het EHRM tot een ander juridisch kader of oordeel komt dan de beide kamers die *Big Brother Watch e.a.* en *Rättvisa* hebben behandeld. Met dit in het achterhoofd, is het niettemin interessant om op dit moment te bezien hoe de Nederlandse regeling van bulkinterceptie en metadata-analyse zich verhoudt tot de door het EHRM geconstateerde knelpunten in de Britse wetgeving en de door het EHRM genoemde waarborgen.

Allereerst is het belangrijk op te merken dat het Straatsburgse Hof met deze uitspraken opnieuw laat zien dat de toepassing van bulkinterceptie noodzakelijk kan zijn in een democratische samenleving.[6] Het was niet vanzelfsprekend dat het EHRM bulkinterceptie als bijzondere bevoegdheid toelaatbaar zou vinden. Dat heeft te maken met de uitspraken in 2014 en 2016 van het Hof van Justitie van de Europese Unie (HvJ EU) met betrekking tot dataretentie, waarin het HvJ EU aangeeft dat een generieke bewaarplicht van telecommunicatiegegevens voor telecomproviders in strijd is met het recht op privacy en de bescherming van persoonsgegevens.[7] Als het EHRM zou aansluiten bij deze lijn

[4] In de Wiv 2017 wordt geen definitie van 'metagegevens' (ook wel 'metadata' genoemd) gegeven. Uit artikel 4 van het Besluit gegevensverstrekking onderzoek van communicatie Wiv 2017 (*Stb*. 2017, 116) kan worden afgeleid dat het bijvoorbeeld gaat om de datum en het tijdstip waarop de verbinding met de gebruiker tot stand is gebracht en beëindigd en de duur van de verbinding, de locatiegegevens van het netwerkaansluitpunt dan wel gegevens betreffende geografische posities van de randapparatuur van een gebruiker en nummers (zoals telefoonnummers of IP-adressen) of technische kenmerken van de randapparatuur van gebruikers die gedurende een bepaalde periode, op een nader aangeduide locatie, verbinding maken of hebben gemaakt met het communicatienetwerk van de aanbieder.

[5] Zie voor een uitgebreide bespreking van beide arresten: EHRM 19 juni 2018, nr. 35252/08, ECLI:CE:ECHR:2018:0913JUD005817013 (*Centrum för Rättvisa t. Zweden*) en EHRM 13 september 2018, nrs. 58170/13, 62322/14 en 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), *EHRC* 2018/208 en 2018/196, m.nt. M. Hagens.

[6] Het EHRM achtte al eerder bulkinterceptie toelaatbaar in *Weber Saravia t. Duitsland* (EHRM 26 juni 2006, nr. 54934/00, ECLI:CE:ECHR:2006:0629DEC005493400, *EHRC* 2007/13, m.nt. J.P. Loof).

[7] HvJ EU 8 april 2014, C293/12, C-594/12, ECLI:EU:C:2014:238, *EHRC* 2014/140, m.nt. M.E. Koning (*Digital Rights t. Ierland*) en HvJ EU 21 december 2016, C-203/15 en C698/15, ECLI:EU:C:2016:970, *EHRC* 2017/79, m.nt.

van het HvJ EU[8] met betrekking tot de grootschalige opslag van gegevens door inlichtingen- en veiligheidsdiensten (ook van personen die niet direct onder de aandacht van de diensten staan), dan had het ook tot de conclusie kunnen komen dat de vergaande bevoegdheid disproportioneel en daarmee niet-noodzakelijk in een democratische samenleving zou zijn. In plaats daarvan legt het EHRM uit dat – mede gezien de hoge dreiging van terroristische aanslagen en technologische ontwikkelingen die het werk van inlichtingen- en veiligheidsdiensten beïnvloeden - aan verdragsstaten een ruime beoordelingsruimte toekomt om te bepalen op welke wijze de nationale veiligheid beschermd moet worden.[9] Daarbij mogen staten ervoor kiezen om bulkinterceptie toe te passen om de onbekende bedreigingen van nationale veiligheid te kunnen identificeren.[10] Het EHRM geeft terecht aan dat de beoordelingsruimte bij de uitvoering van de wet beperkter is dan bij de keuze van de inrichting ervan[11] en dat de inbreuk op de persoonlijke levenssfeer van betrokkenen in de fasen na verwerving (analyseren en gebruiken) het grootst is. Voor die fasen moeten in de wet en de praktijk voldoende waarborgen bestaan.[12]

Ten tweede zijn de arresten *Centrum för Rättvisa* en *Big Brother Watch e.a.* van belang, omdat het EHRM algemene kwalitatieve vereisten formuleert waaraan de nationale wetgeving die bulkinterceptie mogelijk maakt moet voldoen. Deze criteria zijn afgeleid uit het *Roman Zakharov*-arrest,[13] maar aangepast aan bulkinterceptie in het kader van nationale veiligheid (in Nederland dus onderzoeksopdrachtgerichte interceptie genoemd). Het EHRM toetst in de uitspraak met betrekking tot artikel 8 EVRM of de Britse wetgeving voldoet aan de volgende set aan waarborgen: (1) toegankelijkheid van de wetgeving; (2) afbakening toepassingsbereik van *signals intelligence*; (3) de duur, verlenging en beëindiging van de bulkinterceptie; (4) onafhankelijke autorisatie bij onderschepping van de communicatie en voldoende toezicht om effectieve en voortdurende controle op het interceptieproces uit te oefenen; (5) zorgvuldige procedures voor opslag, toegang, onderzoek, gebruik en vernietiging van onderschepte persoonsgegevens; (6) voorwaarden voor het verstrekken van gegevens aan andere inlichtingen- en veiligheidsdiensten en (7) notificatie en voldoende rechtsmiddelen bij het vermoeden van schendingen bij de toepassing van bulkinterceptie.[14]

M.E. Koning (*Tele2 Sverige AB t. Post-och telestyrelsen* en *Secretary of State for the Home Department t. Tom Watson e.a*.).

[8] Bij het HvJ EU is nog een aantal prejudiciële zaken aanhangig m.b.t. de reikwijdte en interpretatie van *Tele2 Sverige/Watson*. Daarbij gaat het bijvoorbeeld om de vraag of de uitspraak zich ook uitstrekt tot de context van nationale veiligheid. Zie *Privacy International t. het VK*, C-623/17 en *French Data Network e.a. t. Frankrijk*, C-512/18 en C-511/18.

[9] Zie over de verhouding tussen *Big Brother Watch e.a.* en de jurisprudentie van het HvJ EU: M. Hagens & C.M.J. Ryngaert, 'Massasurveillance en privacy: De betekenis van het EHRM-arrest Big Brother Watch e.a. t. het Verenigd Koninkrijk voor het EU-recht', *Tijdschrift voor Internetrecht* 2018, afl. 5/6, p. 209-217.

[10] *Big Brother Watch e.a.*, par. 314; *Centrum för Rättvisa*, par. 112. Zie voor deze analyse in soortgelijke bewoordingen: EHRM 13 september 2018, nrs. 58170/13, 62322/14 en 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013, *Computerrecht* 2018/252, m.nt. J.J. Oerlemans (*Big Brother Watch e.a. t. Verenigd Koninkrijk*).

[11] *Big Brother Watch e.a.*, par. 315. Zo ook *Centrum för Rättvisa*, par. 113, *EHRC* 2018/208, m.nt. M. Hagens, par. 10-12.

[12] *Big Brother Watch e.a.*, par. 338.

[13] EHRM 4 december 2015, nr. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, *EHRC* 2016/87, m.nt. M. Hagens, par. 231 (*Roman Zakharov t. Rusland*).

[14] *Big Brother Watch e.a.*, par. 320; *Centrum för Rättvisa*, par. 114 e.v. Zie ook *EHRC* 2018/208, m.nt. M. Hagens, par. 10-12.

Verder benadrukt het EHRM het inbreukmakende karakter van metagegevens van communicatie (*related communications data*) met de overweging dat de verwerking van deze gegevens even, en zo niet meer, ingrijpend kan zijn dan de verwerking van inhoud. Zoals in voetnoot 4 is opgemerkt bevat de Wiv 2017 geen definitie van 'metagegevens' (ook wel 'metadata' genoemd). Metagegevens kunnen in deze context worden gekwalificeerd als gegevens *over* de communicatie, zoals het tijdstip, de datum, de hoeveelheid en duur van de gegevensverzending. Ook het IP-adres, telefoonnummer of ander nummer waarmee verbinding wordt gemaakt en de locatie van het netwerkaansluitpunt dan wel gegevens betreffende geografische posities van de randapparatuur zijn metagegevens. 'Inhoudelijke gegevens' zijn gegevens over de inhoud van communicatie, zoals een gesprek bij een telefoonverbinding of een verstuurd bericht bij e-mail. De verwerking van metagegevens over communicatie wordt door het EHRM dus ook als privacy-intrusief gezien. Deze verwerking vereist passende waarborgen.

> '[T]he content of an electronic communication might be encrypted and, even if it were decrypted, might not reveal anything of note about the sender or recipient. The related communications data, on the other hand, could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with.'[15]

Het EHRM oordeelt in *Big Brother Watch e.a.* onder meer tot een schending van artikel 8 EVRM vanwege (a) het ontbreken van effectief toezicht op het geautomatiseerd doorzoeken van de verworven gegevens aan de hand van selectoren en zoektermen en (b) het ontbreken van effectieve waarborgen met betrekking tot de analyse van de metadata van geïntercepteerde communicatie.[16]

3. Onderzoeksopdrachtgerichte interceptie in de Wiv 2017

Onderzoeksopdrachtgerichte interceptie bestaat uit drie bijzondere bevoegdheden die in de uitoefening behoren tot het vakgebied van s*ignals intelligence* (hierna: sigint). De inlichtingen- en veiligheidsdiensten trachten daarbij relevante informatie te halen uit communicatie die via signalen wordt overgebracht. Vóór de Wiv 2017 hielden de AIVD en MIVD zich ook al bezig met sigint, waarbij de activiteiten zich richtten op het halen van informatie uit de 'ether', zoals satellietverkeer, mobiel telefoonverkeer en radioverkeer.[17] De Wiv 2017 maakt het mogelijk dat de beide diensten nu ook communicatieverkeer op de *kabel*infrastructuur (zoals land- en zeekabels) mogen onderscheppen en analyseren. De noodzaak van deze uitbreiding van ether- naar kabelinterceptie is gelegen in het bijblijven met de ingrijpende wijzigingen in het telecommunicatielandschap in de afgelopen 15 jaar en in het belang van samenwerking tussen inlichtingen- en veiligheidsdiensten.[18]

---

[15] *Big Brother Watch e.a.*, par. 356.
[16] *Big Brother Watch e.a.*, par. 346-347 en 357.
[17] Zie bijvoorbeeld over de inzet van Sigint door de MIVD, CTIVD-rapportnr. 28 (2011) inzake de inzet van Sigint door de MIVD.
[18] Zie voor meer uitleg de memorie van toelichting bij de Wiv 2017, *Kamerstukken II* 2016/17, 34588, 3, p. 8-11 en 91-95. De noodzaak van uitbreiding van bevoegdheden werd onder meer onderschreven door de commissie Dessens die in 2013 de Wiv 2002 evalueerde (Commissie Dessens, *Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, 2013, p. 77, bijlage bij *Kamerstukken II* 2013/14, 33820, 1), alsook door de toezichthouder op de inlichtingen- en veiligheidsdiensten CTIVD (CTIVD, *Eindbalans Wiv 2017: een werkbare wet*, 2018, p. 2).

Bij onderzoeksopdrachtgerichte interceptie worden gegevens (inhoud en metagegevens van communicatie) in grote hoeveelheden (1) onderschept (art. 48 Wiv 2017), (2) geoptimaliseerd (art. 49 Wiv 2017) en (3) nader geanalyseerd (art. 50 Wiv 2017).[19] Bij de analyse van deze gegevens is het mogelijk dat kennis wordt genomen van de inhoud. Daarbij kan gedacht worden aan het uitluisteren van een onderschept telefoongesprek door medewerkers van de AIVD of de MIVD. Het moge duidelijk zijn dat bij het onderscheppen en de analyse van communicatie een ernstige inbreuk op het recht op de persoonlijk levenssfeer van betrokkenen plaatsvindt. Overigens is het goed op te merken dat de ministers in december 2018 lieten weten dat onderzoeksopdrachtgerichte interceptie op de kabel in de praktijk nog niet plaatsvindt.[20]

In deze paragraaf gaan we kort in op de wijze waarop de interceptiebevoegdheid (art. 48 Wiv 2017) bij onderzoeksopdrachtgerichte interceptie en het proces van optimalisatie van de interceptie (art. 49 lid 1 Wiv 2017) in de Nederlandse wet is geregeld. Ook adresseren we het eerste geconstateerde knelpunt in de *Big Brother Watch*-zaak over toezicht bij het analyseren van de verworven gegevens aan de hand van selectoren en zoektermen. In Nederland noemen we dit proces 'selectie', hetgeen is geregeld als een aparte bijzondere bevoegdheid in artikel 50 lid 1 sub a Wiv 2017. Ter uitvoering van de bijzondere bevoegdheid tot selectie kunnen selectiecriteria worden vastgesteld. Deze selectiecriteria zien bijvoorbeeld op technische kenmerken van personen, organisaties en/of aan een nader omschreven onderwerp gerelateerde trefwoorden.[21] Een technisch kenmerk – in het Engels ook wel *selector* genoemd – betreft bijvoorbeeld een telefoonnummer, e-mailadres en IP-adres.[22] In paragraaf 4 wordt het tweede knelpunt uit de *Big Brother Watch*-zaak geadresseerd over waarborgen bij de analyse van de metadata van geïntercepteerde communicatie. In Nederland is dit geregeld als de bijzondere bevoegdheid tot 'geautomatiseerde data-analyse' in artikel 50 lid 1 sub b Wiv 2017.

De naam 'onderzoeksopdrachtgerichte interceptie'

Het stelsel van *onderzoeksopdrachtgerichte* interceptie ontleent zijn naam aan de Geïntegreerde Aanwijzing inlichtingen- en veiligheidsdiensten. In deze aanwijzing staan de zogenoemde 'onderzoeksopdrachten' die zijn geformuleerd door 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).[23] De precieze inhoud van de Geïntegreerde Aanwijzing inlichtingen- en veiligheidsdiensten is staatsgeheim. In de memorie van toelichting bij de Wiv 2017 worden wel de volgende drie voorbeelden genoemd: (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.[24]

[19] Zie voor een uitgebreide bespreking van het stelsel van onderzoeksopdrachtgerichte interceptie ook: P.J.F. Koop, 'De Snowden-onthullingen en ongerichte interceptie onder de Wiv 2017', *Justitiële verkenningen* 2018, nr. 1, p. 133-147 en J.J. Oerlemans & M. Hagens, 'De Wet op de inlichtingen- en veiligheidsdiensten 2017: een technologisch gedreven wet', *Computerrecht* 2018/111, nr. 3, p. 130-141.

[20] Aanbiedingsbrief voortgangsrapportage CTIVD nr. 59 aan de Tweede Kamer over de werking van de Wiv 2017, 4 december 2018, p. 3, *Kamerstukken II* 2018/19, 34588, 80.

[21] *Kamerstukken II* 2016/17, 34588, 3, p. 108.

[22] *Kamerstukken II* 2016/17, 34588, 3, p. 106.

[23] Zie de Geïntegreerde Aanwijzing Inlichtingen en Veiligheid 2019-2022, *Stcrt.* 2018, 68088. Op het instrument van de Geïntegreerde Aanwijzing is kritiek geleverd, omdat daarmee mogelijk te veel politieke invloed wordt uitgeoefend op het werk van de diensten, zie oratie P.H.A.M. Abels, *Per undas adversas? Geheime diensten in de maalstroom van politiek en beleid* (oratie Universiteit Leiden), 2018.

[24] *Kamerstukken II* 2016/17, 34588, 3, p. 16.

Waarborgen bij de interceptie van gegevens en optimalisatie van de interceptie
Voorafgaand aan de interceptie van communicatie gaan de AIVD en de MIVD na op welk toegangspunt zij het beste de interceptie in de ether of op de kabel kunnen inzetten. Daarbij gaan de diensten bijvoorbeeld na op welke satelliet, radiofrequentie of *fiber* op een glasvezelkabel zij zich moeten richten om de meeste relevante gegevens te verzamelen om te voldoen aan de vooraf bepaalde onderzoeksopdrachten.[25] Vervolgens wordt een aanvraag gedaan voor de interceptie van communicatieverkeer op grond van artikel 48 Wiv 2017.

In de aanvraag voor de toepassing van de bevoegdheid in artikel 48 Wiv 2017 dient genoemd te worden voor welke onderzoeksopdracht de bevoegdheid wordt ingezet (en welke noodzaak daartoe bestaat), waarom de inzet proportioneel is (de verhouding tussen de noodzaak een bevoegdheid in te zetten en de privacy-inmenging van de betrokkene), waarom de inzet subsidiair is (er zijn geen minder vergaande onderzoeksmiddelen om hetzelfde doel te bereiken) en waarom de inzet 'zo gericht mogelijk' is. Het gerichtheidsvereiste is naar aanleiding van de motie Recourt[26] geïntroduceerd voor alle (bijzondere) bevoegdheden en vervolgens vastgelegd in artikel 5 Beleidsregels Wiv 2017.[27] De verwachting is dat het vereiste wordt gecodificeerd in de Wiv 2017 door de Wijzigingswet Wiv 2017.[28] Helaas maakt de wetgever in de beschikbare stukken niet duidelijk wat wordt bedoeld met 'zo gericht mogelijk', maar in de context van artikel 48 Wiv 2017 moet in ieder geval worden nagegaan hoe bij de inzet zo relevant mogelijke gegevens worden onderschept.

In het proces van het onderscheppen van het communicatieverkeer gaan de AIVD en MIVD constant na of het verkeer dat wordt onderschept, het verkeer is waar ze naar op zoek zijn. Voor dit proces van 'search gericht op interceptie'[29] wordt bijvoorbeeld bij de interceptie van radioverkeer af en toe op een andere frequentie afgestemd, om te bezien of over die frequentie relevant communicatieverkeer gaat. Dit proces is ook apart geregeld in artikel 49 lid 1 Wiv 2017.

Voor de interceptie van telecommunicatieverkeer ten behoeve van de uitoefening van onderzoeksopdrachtgerichte interceptie en de optimalisatie van het search-proces moet een aanvraag worden gedaan op grond van artikel 48 jo. artikel 49 lid 1 Wiv 2017. De minister van Binnenlandse Zaken of de minister van Defensie geeft vervolgens al dan niet toestemming voor de inzet van de bijzondere bevoegdheden. Vervolgens moet de Toetsingscommissie Inzet Bevoegdheden (hierna: TIB) toestemming geven voordat dat de interceptie daadwerkelijk plaats mag vinden.[30]

Op de uitvoering van de inzet van deze bijzondere bevoegdheid houdt de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (hierna: CTIVD) toezicht. De Tweede Kamer en de ministers hebben de CTIVD nadrukkelijk gevraagd toezicht te houden op en te rapporteren over (bepaalde aspecten van) de uitoefening van onderzoeksopdrachtgerichte interceptie door de AIVD en de MIVD in de aanloop naar de vervroegde evaluatie van de wet (start uiterlijk binnen twee jaar na

[25] *Kamerstukken II* 2016/17, 34588, 3, p. 103-104 en p. 110.
[26] *Kamerstukken II* 2016/17, 34588, 66.
[27] *Kamerstukken II* 2017/18, 34588, 76, bijlage.
[28] Zie conceptwetsvoorstel Wijziging Wiv 2017. Beschikbaar op: www.internetconsultatie.nl/wiv2017 (laatst geraadpleegd op 21 maart 2019). Het wetsvoorstel wordt naar verwachting op korte termijn naar de Tweede Kamer gestuurd.
[29] Zie *Kamerstukken II* 2016/17, 34588, 3, p. 103-105.
[30] De TIB is nieuw in de Wiv 2017. De eerste resultaten van de toetsing van de TIB zijn te lezen in de voortgangsbrief die de TIB in oktober 2018 uitbracht, zie www.tib-ivd.nl.

inwerkingtreding).[31] De CTIVD voert op het moment van schrijven (februari 2019) twee diepteonderzoeken uit naar dit onderwerp.[32] In de voortgangsrapportage van november 2018 aan de Tweede Kamer over de werking van de Wiv 2017 heeft de CTIVD zich al kritisch uitgelaten over het gebrek aan beleid en werkinstructies die zien op de uitvoering van het gerichtheidsvereiste en datareductie bij onderzoeksopdrachtgerichte interceptie.[33]

Voldoende toezicht bij selectie

Op de opgeslagen gegevens[34] mogen de AIVD en MIVD zogenoemd 'selectie' plegen. Zoals eerder is aangegeven is het uitoefenen van selectie geregeld als een bijzondere bevoegdheid in artikel 50 lid 1 sub a Wiv 2017. Selectie van gegevens vindt plaats met het oogmerk om van de *inhoud* van de geselecteerde gegevens kennis te kunnen nemen, zoals het uitluisteren van een onderschept telefoongesprek. Ter uitvoering van de bijzondere bevoegdheid tot selectie worden selectiecriteria gebruikt, zoals een telefoonnummer, IP-adres of e-mailadres die bij een persoon of organisatie hoort.

Voor de inzet van de bijzondere bevoegdheid tot selectie is toestemming van de minister van Binnenlandse Zaken of de minister van Defensie vereist. Ook de TIB moet voor de inzet ervan de toestemming van de minister rechtmatig verklaren en de CTIVD houdt achteraf toezicht op een rechtmatige inzet van de bijzondere bevoegdheid. De toestemming voor selectie wordt voor een periode van ten hoogste drie maanden verleend en telkens op een daartoe strekkend verzoek verlengd. Het verzoek bevat de identiteit van de persoon of organisatie of een omschrijving van het onderwerp ten aanzien waarvan de bevoegdheid moet worden toegepast.

Op grond van het bovenstaande concluderen wij dat van effectief toezicht op het geautomatiseerd doorzoeken van de verworven gegevens aan de hand van selectoren en zoektermen in Nederland sprake lijkt te zijn. In de Wiv 2017 is voor onderzoeksopdrachtgerichte interceptie gekozen voor een getrapt regime, waarbij voor (1) de interceptie van de communicatie, (2) de optimalisatie van het proces en (3) de analyse van de communicatie telkens afzonderlijk toestemming moet worden gevraagd aan de betrokken minister en de TIB. Telkens moet daarbij de noodzaak, proportionaliteit, subsidiariteit en gerichtheid worden gemotiveerd. Achteraf houdt de CTIVD toezicht op een rechtmatige toepassing. Daarmee lijkt een belangrijk kritiekpunt van het EHRM in *Big Brother Watch e.a.*, namelijk het ontbreken van effectief toezicht op het geautomatiseerd doorzoeken van de verworven gegevens aan de hand van selectoren en zoektermen, in het Nederlandse stelsel te zijn ondervangen.

[31] Brief van de ministers van BZK en Defensie, 25 april 2018, *Kamerstukken II* 2017/18, 34588, 76 (bijlage).
[32] Aankondiging in december 2018 van onderzoeken naar toepassing van filters en de wijze van selectie, zie www.ctivd.nl/actueel/nieuws/2018/12/05/index (laatst geraadpleegd op 21 maart 2019).
[33] CTIVD-rapport nr. 59 (2018), *Kamerstukken II* 2018/19, 34588, 80 (bijlage).
[34] Art. 48 lid 5 Wiv 2017. De onderschepte gegevens uit onderzoeksopdrachtgerichte interceptie mogen maximaal drie jaar worden bewaard. Niet-relevante gegevens moeten na analyse terstond worden vernietigd. Het gaat daarbij om gegevens die voor het onderzoek én andere onderzoeken van de AIVD of de MIVD niet relevant zijn. Bij kabelverkeer moet elk jaar worden nagegaan of het noodzakelijk is de gegevens nog langer te bewaren (zie Kamerbrief van 6 april 2018 van de minister van BZK en de minister van Defensie, *Kamerstukken II* 2017/18, 34588, 70) naar aanleiding van de uitslag van het raadgevend referendum.

4. Geautomatiseerde data-analyse

In de *Big Brother Watch*-zaak constateerde het EHRM een schending van artikel 8 EVRM omdat de metadata uit bulkinterceptie zonder restricties konden worden onderzocht door medewerkers van de Britse communicatie-inlichtingendienst.[35]

Het EHRM legt goed uit dat de analyse van metadata een zware inmenging met het recht op privacy van de betrokkenen kan inhouden. De reden is dat metadata gevoelig kan zijn, omdat het onder meer informatie kan bevatten over de identiteit van beide communicerende partijen, hun geolocatie en gebruikte apparatuur. Bij de opslag en analyse van deze gegevens in bulk wordt de inmenging met het recht op privacy groter, omdat het daarmee mogelijk is de contacten van een persoon, bewegingen en locaties, internetgeschiedenis en communicatiepatronen in kaart te brengen.[36] Het Verenigd Koninkrijk heeft volgens het EHRM geen juiste balans tussen het belang van bescherming van de nationale veiligheid en eerbiediging van het recht van privacy getroffen door deze categorie van gegevens uit te sluiten van de waarborgen in de wetgeving.[37]

In Nederland is 'geautomatiseerde data-analyse' (metadata-analyse) op geïntercepteerde communicatie uit bulkinterceptie een bijzondere bevoegdheid met specifieke waarborgen.[38] In de Wiv 2002 werd de analyse van metadata niet geregeld. Het belang van een wettelijke regeling met waarborgen werd zowel door de CTIVD als de Commissie evaluatie Wiv 2002 (Commissie Dessens) benadrukt.[39] De regeling is complex en vergt nadere toelichting.

Artikel 50 lid 1 sub b Wiv 2017 biedt de grondslag voor de bijzondere bevoegdheid voor geautomatiseerde data-analyse in het kader van onderzoeksopdrachtgerichte interceptie. Toestemming van de minister en de TIB zijn vereist wanneer metadata verkregen uit onderzoeksopdrachtgerichte interceptie wordt betrokken in de geautomatiseerde data-analyse en de analyse is gericht op het identificeren van personen of organisaties (art. 50 lid 4 Wiv 2017). Een voorbeeld hiervan is het op basis van metadata in kaart brengen van iemands netwerk (*contact chaining*) met het doel om personen of organisaties te identificeren.[40]

Bovendien stelt artikel 50 lid 4 Wiv 2017 extra eisen aan het verzoek om toestemming, naast de standaard vereisten zoals noodzakelijkheid, proportionaliteit, subsidiariteit en gerichtheid in artikel 26 en 29 Wiv 2017. In artikel 50 lid 4 wordt doorverwezen naar artikel 60 Wiv 2017. Op grond van dit artikel moet de aanvraag ook (a) een aanduiding bevatten van de toe te passen vorm van geautomatiseerde data-analyse en (b) een aanduiding van de gegevensbestanden die in de geautomatiseerde data-analyse worden betrokken (voor zover van toepassing).[41]

---

[35] *Big Brother Watch e.a.*, par. 355.
[36] *Big Brother Watch e.a.*, par. 353-355.
[37] *Big Brother Watch e.a.*, par. 357.
[38] Zie art. 50 lid 1 sub b jo lid 4 jo artikel 60 Wiv 2017.
[39] Commissie Dessens, *Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, 2013 en CTIVD-rapport nr. 38 (2014) over gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD.
[40] Afkomstig uit de Rechtseenheidsbrief TIB en CTIVD van 23 november 2018 aan de Eerste en Tweede Kamer over geautomatiseerde data-analyse ex art. 50 Wiv 2017, p. 2, *Kamerstukken II* 2018/19, 29924, 174. Beschikbaar op: https://www.ctivd.nl/documenten/brieven/2018/11/23/index1 (laatst geraadpleegd op 21 maart 2019).
[41] In art. 60 Wiv 2017 wordt geautomatiseerde data-analyse kort gezegd beschreven als het geautomatiseerd verwerken van gegevens, onder meer door deze op geautomatiseerde wijze onderling of in combinatie met elkaar te vergelijken, te doorzoeken aan de hand van profielen, of te vergelijken met het oog op het opsporen van bepaalde patronen. Deze uitleg geeft een niet-limitatieve opsomming van vormen van geautomatiseerde

In Nederland is dus - in tegenstelling tot het Verenigd Koninkrijk - voor geautomatiseerde data-analyse op gegevens uit onderzoeksopdrachtgerichte interceptie een bijzondere bevoegdheid van toepassing, met een aparte toets en toestemming door de minister en de TIB als dat gericht is op de identificatie van personen en organisaties. Nederland biedt op dit punt dus aanzienlijk meer bescherming aan betrokkenen vergeleken met het Verenigd Koninkrijk en heeft er in de Wiv 2017 goed aan gedaan deze regeling te treffen voor geautomatiseerde data-analyse.

5. De beperkte reikwijdte van de waarborgen voor geautomatiseerde data-analyse

Het is de vraag of de Wiv 2017 een voldoende dekkende regeling voor geautomatiseerde data-analyse biedt. De oplettende lezer is opgevallen dat de bijzondere bevoegdheid van artikel 50 Wiv 2017 slechts geldt voor metadata-analyse van gegevens uit de bevoegdheid van onderzoeksopdrachtgerichte interceptie en *niet bij andere bevoegdheden*.

De CTIVD en de TIB hebben in het kader van rechtseenheid benadrukt dat de mate van inmenging in grondrechten leidend is voor het systeem van toezicht en waarborgen (zoals ministeriële toestemming en toetsing door de TIB) dat volgens het EHRM bij de verwerking van bulkgegevens van toepassing hoort te zijn. De TIB en de CTIVD achten ook het huidige onderscheid naar de oorsprong van de gegevens (gegevens uit art. 48 Wiv 2017 (onderzoeksopdrachtgerichte interceptie)) niet wenselijk. De gegevens kunnen bijvoorbeeld ook afkomstig zijn uit toepassing van de hackbevoegdheid (art. 45 Wiv 2017), waarop vervolgens geautomatiseerde data-analyse kan worden toegepast die een ernstige inbreuk op het privéleven van betrokkenen inhoudt. De TIB en de CTIVD geven daarom aan dat het wenselijk is de regeling in de Wiv 2017 op het terrein van geautomatiseerde data-analyse aan te passen.[42]

In hun reactie (19 maart 2019) op de rechtseenheidbrief van de TIB en de CTIVD geven de ministers van BZK en Defensie aan dat de wet op dit moment niet wordt aangepast in het voorstel tot de Wijzigingswet Wiv 2017 die binnenkort aan de Tweede Kamer wordt aangeboden.[43] De ministers achten de waarborg van ministeriële toestemming slechts gepast bij geautomatiseerde data-analyses die een 'substantiële privacy-inbreuk' met zich meebrengen. Als voorbeeld van een vorm van geautomatiseerde data-analyse die meer inbreuk maakt op de persoonlijke levenssfeer wordt in de brief genoemd 'het geautomatiseerd analyseren van gegevensbestanden met als resultaat het weergeven van potentiële verbanden en patronen tussen personen'. Als voorbeeld van een beperkte inbreuk wordt gegeven 'het invoeren van een telefoonnummer in een applicatie die vervolgens de telefoonnummers weergeeft waarmee het ingevoerde telefoonnummer verbinding heeft gehad'. Volgens de ministers is voor deze laatste vorm van geautomatiseerde data-analyse toestemming van de minister en toetsing door de TIB niet passend.

De huidige wet schrijft echter voor dat voor geautomatiseerde data-analyse van gegevens afkomstig uit onderzoeksopdrachtgerichte interceptie dat gericht is op de identificatie van personen of organisatie toestemming van de minister en toetsing van de TIB noodzakelijk is. Het tweede voorbeeld van geautomatiseerde data-analyse valt mogelijk binnen de reikwijdte van art. 50 lid 1 sub b jo lid 4 Wiv 2017. Bovendien is het de vraag of het blootleggen van alle telefoonnummers waarmee

---

data-analyse. Er gelden geen bijzondere toestemmingsvereisten voor deze analyses. Het bevorderen of treffen van maatregelen jegens een persoon uitsluitend op basis van de resultaten van een geautomatiseerde data-analyse niet toegestaan.

[42] Zie de Rechtseenheidsbrief TIB en CTIVD van 23 november 2018 aan de Eerste en Tweede Kamer over geautomatiseerde data-analyse ex art. 50 Wiv 2017, p. 6, *Kamerstukken II* 2018/19, 29924, 174.

[43] Afschrift van de brief aan de CTIVD en de TIB met reactie op de rechtseenheidsbrieven van 19 maart 2019, *Kamerstukken II* 2018/19, 29924, 179.

een persoon contact heeft gehad wel als een 'geringe inbreuk op het recht op de persoonlijke levenssfeer' kan worden gezien. Uit de brief wordt verder niet duidelijk of de ministers de toepassing van de bijzondere bevoegdheid voor geautomatiseerde data-analyse slechts toepasselijk vinden voor zover de gegevens afkomstig zijn uit onderzoeksopdrachtgerichte interceptie.

Kortom, er bestaat onduidelijkheid over de vraag wat geautomatiseerde data-analyses precies zijn die een substantiële privacy-inbreuk met zich meebrengen en hoe het gebruik van dit criterium zich met de huidige wet verhoudt. Deze onduidelijkheid is onwenselijk en daarom hebben de TIB en CTIVD de beide diensten opgeroepen duidelijkheid op dit punt te verschaffen.[44] De CTIVD voert in het kader van het onderzoek naar de werking van de Wiv 2017 een nulmeting uit naar geautomatiseerde data-analyse waarover de Tweede Kamer in 2019 wordt geïnformeerd.[45] De uitwerking van de nieuwe regelingen in de Wiv 2017 moeten dus verder uitkristalliseren. Het is hierbij goed in het achterhoofd te houden dat het EHRM in *Centrum för Rättvisa* en *Big Brother Watch e.a.* uitdrukkelijk overweegt dat de regelingen met waarborgen ook in de praktijk hun uitwerking moeten krijgen en niet alleen op papier hun betekenis hebben:

> '(…) while the Court considers judicial authorisation to be an important safeguard, and perhaps even "best practice", by itself it can neither be necessary nor sufficient to ensure compliance with Article 8 of the Convention (…). Rather, regard must be had to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse'.[46]

In dat kader zijn ook aanvullende waarborgen bij GDA van belang, zoals functie- en taakscheiding van medewerkers die intrusieve geautomatiseerde data-analyses mogen uitvoeren en een strikt stelsel van interne logging en controle. Met behulp van logging kan worden nagegaan welke medewerkers metadata-analyses op een bepaald moment hebben uitgevoerd. Controle op de rechtmatigheid van die verwerking kan plaatsvinden door de diensten zelf en de CTIVD. Het fungeert als waarborg als slechts bepaalde medewerkers met een bepaalde functie geautoriseerd zijn voor privacy-intrusieve data-analyses. De huidige Wiv 2017 stelt deze functie-taakscheiding bij intrusieve vormen van geautomatiseerde data-analyse van gegevens overigens niet verplicht.

6. Conclusie

De Wiv 2017 geeft de AIVD en de MIVD verschillende mogelijkheden om een grote hoeveelheid van gegevens (bulk) te verwerven en te verwerken ten behoeve van hun taakuitoefening. In aanloop van het referendum lag daarbij vooral de nadruk op onderzoeksopdrachtgerichte interceptie. Daarom werd de nieuwe Wiv steevast 'sleepwet' genoemd.

In dit artikel zijn de 'bulkbevoegdheden' van onderzoeksopdrachtgerichte interceptie en geautomatiseerde data-analyse in verhouding met het recht op privacy onderzocht. Uit jurisprudentie blijkt dat het EHRM bepaalde kwalitatieve vereisten stelt aan de nationale wetgeving van verdragsstaten, waaronder Nederland.

---

[44] Zie de Rechtseenheidsbrief TIB en CTIVD van 23 november 2018 aan de Eerste en Tweede Kamer over geautomatiseerde data-analyse ex art. 50 Wiv 2017, p. 3, *Kamerstukken II* 2018/19, 29924, 174. Beschikbaar op www.ctivd.nl/documenten/brieven/2018/11/23/index1 (laatst geraadpleegd op 21 maart 2019).

[45] Brief van de CTIVD aan de Tweede Kamer, 26 april 2018, over de toezichtsactiviteiten naar de werking van de Wiv 2017, *Kamerstukken II* 2017/18, 34588, 77. Beschikbaar op www.ctivd.nl/documenten/brieven/2018/04/30/index (laatst geraadpleegd op 21 maart 2019).

[46] *Big Brother Watch e.a.,* par. 320.

Voor onderzoeksopdrachtgerichte interceptie biedt de Wiv 2017 strenge waarborgen, waaronder het getrapte systeem van voorafgaande toestemming door de minister en de TIB voor de interceptie zelf, de optimalisatie van het interceptieproces en de nadere analyse van de onderschepte gegevens uit interceptie. Het systeem voldoet daarmee aan een belangrijk kritiekpunt in de *Big Brother Watch*-zaak over voorafgaande toestemming en toezicht op de nadere analyse van de gegevens met het oogmerk om kennis te nemen van de inhoud (het selectieproces).

Een knelpunt bestaat echter met betrekking tot de beperkte reikwijdte van de regeling voor de bijzondere bevoegdheid tot geautomatiseerde data-analyse. De bijzondere bevoegdheid geldt slechts voor de metadata-analyse van gegevens uit onderzoeksopdrachtgerichte interceptie (en geen andere bevoegdheden) met het doel om personen of organisaties te identificeren (en niet voor andere doelen). Het is daarmee niet gezegd dat de Nederlandse regeling in strijd is met artikel 8 EVRM, maar het moet wel op zijn minst duidelijk zijn welke data-analyses precies onder de regeling vallen en welke waarborgen voor data-analyses worden toegepast die buiten de regeling vallen. Tot dusver is dit nog onduidelijk. Geautomatiseerde data-analyse is om deze reden een onderwerp dat de gemoederen in het inlichtingendomein voorlopig zal blijven bezighouden.