Universiteit Utrecht

Geautomatiseerde data-analyse door inlichtingen- en veiligheidsdiensten

Preadvies Staatsrechtconferentie 2020

Jan-Jaap Oerlemans[1]

[1] Prof. mr. dr. J.J. Oerlemans is bijzonder hoogleraar Inlichtingen en Recht bij de Universiteit Utrecht. Hij is verbonden aan het Montaigne Centrum voor Rechtsstaat en Rechtspleging en het Willem Pompe Instituut voor Strafrechtwetenschappen. Oerlemans is tevens senior onderzoeker bij de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD).

1. Inleiding

'Metadata-analyse' is een vorm van geautomatiseerde data-analyse die inlichtingen- en veiligheidsdiensten voornamelijk gebruiken om nieuwe 'targets' te identificeren. Targets zijn personen die bij inlichtingen- en veiligheidsdiensten onder de aandacht staan, meestal omdat zij een bedreiging voor de nationale veiligheid vormen. In 2013 legde de toenmalige minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) uit dat metadata-analyse in essentie inhoudt dat de telefoonnummers van gekende terroristen worden vergeleken met de bulk aan metagegevens om te bezien of een persoon die nog niet onder de aandacht van de dienst staat, in dezelfde cirkel opduikt als de gekende terroristen.[2] Het gaat in dat geval over het 'kennen van de ongekende dreiging' door mogelijke terroristen te identificeren die een gevaar kunnen vormen voor de nationale veiligheid van Nederland.[3]

In Nederland en in het buitenland is veel maatschappelijke discussie geweest over metadata-analyse als vorm van geautomatiseerde data-analyse. Dat is niet in de laatste plaats vanwege de onthullingen in juni 2013 van Edward Snowden over de afluisterpraktijken van de Amerikaanse communicatie-inlichtingendienst, de National Security Agency (NSA).[4] Door middel van 'metadata-analyse' op telefonieverkeer is het bijvoorbeeld mogelijk na te gaan wie met wie belt, op welk tijdstip, met een indicatie van de locatie waar de verbinding vandaan komt. Metadata zijn gegevens die *niet* over de inhoud van gegevens gaan, zoals de inhoud van een telefoongesprek of een e-mailbericht.[5] Toch kan de privacy-inbreuk even groot of zelfs groter zijn bij metadata-analyse vergeleken met het kennisnemen van de inhoud van communicatie.[6] Vergelijk bijvoorbeeld de privacy-inbreuk van de kennisname van de inhoud van een zakelijk telefoongesprek met een metadata-analyse van het surfgedrag van een persoon.

Metadata-analyse is in de Wet op de inlichtingen- en veiligheidsdiensten (hierna: Wiv) lange tijd "lastenvrij" geweest, zonder een specifieke wettelijke regeling met waarborgen om de rechten en vrijheden van betrokkenen extra te beschermen. In de Wiv 2017 is metadata-analyse per 1 maart 2018 geregeld als een zogenoemde 'bijzondere bevoegdheid'. Dat betekent dat een gedetailleerde regeling met zware eisen geldt voor de inzet van het inlichtingenmiddel, met voorafgaande toestemming van de minister en een rechtmatigheidstoets van de Toetsingscommissie Inzet Bevoegdheden (TIB).[7]

Het probleem is dat deze nieuwe bijzondere bevoegdheid voor metadata-analyse in de praktijk nauwelijks wordt toegepast, namelijk alleen voor het doeleinde van 'force protection'.[8] Force protection gaat over de bescherming van militairen in missiegebieden, zoals het identificeren en lokaliseren van vijandelijke eenheden.[9] Deze beperkte toepassing van de bijzondere bevoegdheid is onwenselijk, omdat metadata-analyse een belangrijk instrument is voor de bescherming van de nationale veiligheid. De bijzondere bevoegdheden zijn in de Wiv 2017 gecreëerd als instrument voor de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en

[2] *Kamerstukken II* 2012/13, 30977, nr. 71.
[3] Zie *Kamerstukken II* 2016/17, 34588, nr. 3, p. 93.
[4] Zie bijvoorbeeld *Kamerstukken II* 2012/13, 30977, nr. 56 (Kamerbrief van 21 juni 2013 over hoe de wettelijke bevoegdheden van de Nederlandse inlichtingen- en veiligheidsdiensten zich verhouden tot het zogeheten PRISM-programma of vergelijkbare methoden van informatievergaring). Zie naar aanleiding van dit debat ook CTIVD-rapport nr. 38 (2014) over gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD (hierna: CTIVD-rapport nr. 38).
[5] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 111. Zie ook paragraaf 2.1 meer uitgebreide toelichting over het begrip metadata.
[6] Zie bijvoorbeeld HvJ EU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238, par. 27 (*Digital Rights t. Ierland*) en EHRM 13 september 2018, nrs. 58170/13, 62322/14, 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013, par. 356-357 (*Big Brother Watch e.a.t. het Verenigd Koninkrijk*) (sinds februari 2019 aanhangig bij de Grote Kamer).
[7] Zie artikel 50 lid 1 sub a Wiv 2017. Op 1 maart 2018 is de Wet op de inlichtingen- en veiligheidsdiensten 2017 in werking getreden. *Kamerstukken II* 2017/18, 34588, nr. 70.
[8] Zie CTIVD-rapport nr. 62 (2019) en 69 (2020) (Voortgangsrapportage II en IV Implementatie Wiv 2017).
[9] Zie bijvoorbeeld CTIVD-rapport nr. 44 (2015) over MIVD-operaties op het gebied van piraterijbestrijding in de Hoorn van Afrika.

Veiligheidsdienst (MIVD) voor hun taakuitvoering in het kader van de nationale veiligheid. Dat is naast force protection - waar alleen de MIVD zich mee bezighoudt - bijvoorbeeld ook de bescherming van de nationale veiligheid door het produceren van inlichtingen over jihadistisch terrorisme of het tegengaan van digitale spionage door Rusland en China.[10] Als deze bevoegdheid in de praktijk niet of slechts heel beperkt wordt gebruikt, kan dit ten koste gaan van die belangrijke taakuitoefening.

Dit preadvies gaat over de vraag hoe metadata-analyse, als vorm van geautomatiseerde data-analyse, beter kan worden geregeld in de Wiv. Geautomatiseerde data-analyse speelt een belangrijke rol in modern inlichtingenwerk.[11] De regeling moet voldoende 'werkbaar' zijn voor de AIVD en de MIVD en voldoende waarborgen bieden ter bescherming van de fundamentele rechten van de betrokkene. De Commissie-Jones-Bos is bovendien op 17 april 2020 aangesteld om de Wiv 2017 te evalueren en daarover een rapport met aanbevelingen uit te brengen. De evaluatiecommissie is verzocht te rapporteren over verschillende onderwerpen die in dit preadvies aan bod komen, zoals over de knelpunten in de toepassingspraktijk van de wet. Ten tijde van het verschijnen van dit preadvies is het rapport van de evaluatiecommissie nog niet gepubliceerd. De voorstellen in dit preadvies kunnen bijdragen aan het vinden van een regeling die zowel werkbaar is in de praktijk, als voldoende waarborgen bieden ter bescherming van de fundamentele rechten van de betrokken personen.

Om te bepalen aan welke kwalitatieve de Wiv 2017 moet voldoen, toets ik in dit preadvies aan jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) en het Hof van Justitie van de EU (HvJ EU). De gegevensverwerkingsbepalingen uit de Wiv 2017 worden niet tegen de lat van de algemene verordening gegevensverwerking (AVG)[12] en de richtlijn gegevensbescherming opsporing en vervolging[13] gehouden, omdat deze niet toepassing zijn op de inlichtingen- en veiligheidsdiensten. Wel blijkt uit dit preadvies dat enkele bepalingen uit de Wiv 2017 zijn geïnspireerd op deze EU-wetgeving.

Het preadvies is als volgt opgebouwd. In paragraaf 2 wordt eerst de regeling voor metadata-analyse uit bulkinterceptie besproken en de problemen met de huidige regeling geïdentificeerd. Paragraaf 3 gaat na hoe de algemene bepalingen omtrent gegevensverwerking in de Wiv 2017 metadata-analyse en geautomatiseerde data-analyse normeren en welke minimale vereisten voor de nationale wetgeving kunnen worden afgeleid uit de jurisprudentie. Paragraaf 4 en paragraaf 5 bespreken twee oplossingsrichtingen om metadata-analyse beter te regelen en welke aandachtspunten de wetgever daarbij in het achterhoofd moet houden. Het preadvies sluit af met een conclusie.

2. Metadata-analyse in artikel 50

Voor metadata-analyse die wordt uitgevoerd na de inzet van onderzoeksopdrachtgerichte interceptie (artikel 48 Wiv 2017) (hierna: bulkinterceptie) moet een bijzondere bevoegdheid worden ingezet (artikel 50 lid 1 sub b Wiv 2017). In de memorie van toelichting van de Wiv 2017 wordt het proces van metadata-analyse toegelicht. Uitgelegd wordt dat aan de hand van metadata kan worden vastgesteld of 'tussen telefoontoestellen contact is geweest, of e-mailadressen met elkaar verband houden, of IP-adressen met elkaar in contact staan en wanneer dat heeft plaatsgevonden, welke websites vanaf een PC zijn bezocht, of waar een communicatiemiddel zich

[10] Zie bijvoorbeeld het jaarverslag 2019 van de AIVD en de MIVD.
[11] Zie, o.a., ook B.G.J. de Graaff, *Data en dreiging. Stap in de wereld van intelligence*, Amsterdam: Boom 2019.
[12] Verordening (EU) 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), PbEU 2016, L 119.
[13] Richtlijn (EU) 2016/680 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ, PbEU 2016, L119.

op een bepaald moment bevond.' Door deze gegevens uit bulkinterceptie te combineren met gegevens uit andere bronnen kan een 'beeld kan worden verkregen omtrent zijn relatienetwerk en verplaatsingsgedrag'.[14] Metadata-analyse kan dus informatie opleveren over de bekende targets en over andere, nog onbekende targets. Niet alle analyses dienen om nieuwe targets te identificeren. De analyse kan ook dienen om een verplaatsing van een target vast te stellen of meer te leren over het surfgedrag van een target. Het gaat daarbij niet alleen om het analyseren van communicatieverkeer uit telefonie, maar ook internetverkeer.[15]

In CTIVD-rapport nr. 38 (2014) over gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD, wordt het gegevensverwerkingsproces iets uitgebreider toegelicht. Daarin is te lezen dat de metagegevens worden samengevoegd uit verschillende bronnen en met behulp van applicaties worden geanalyseerd. Destijds ging het daarbij om (1) analyseapplicaties 'ten behoeve van naslag in geïntegreerde gegevensbronnen', (2) analyseapplicaties ten behoeve van netwerkanalyse en (3) analyseapplicaties die gebruik maken van uitgebreide visualisatietechnieken.[16]

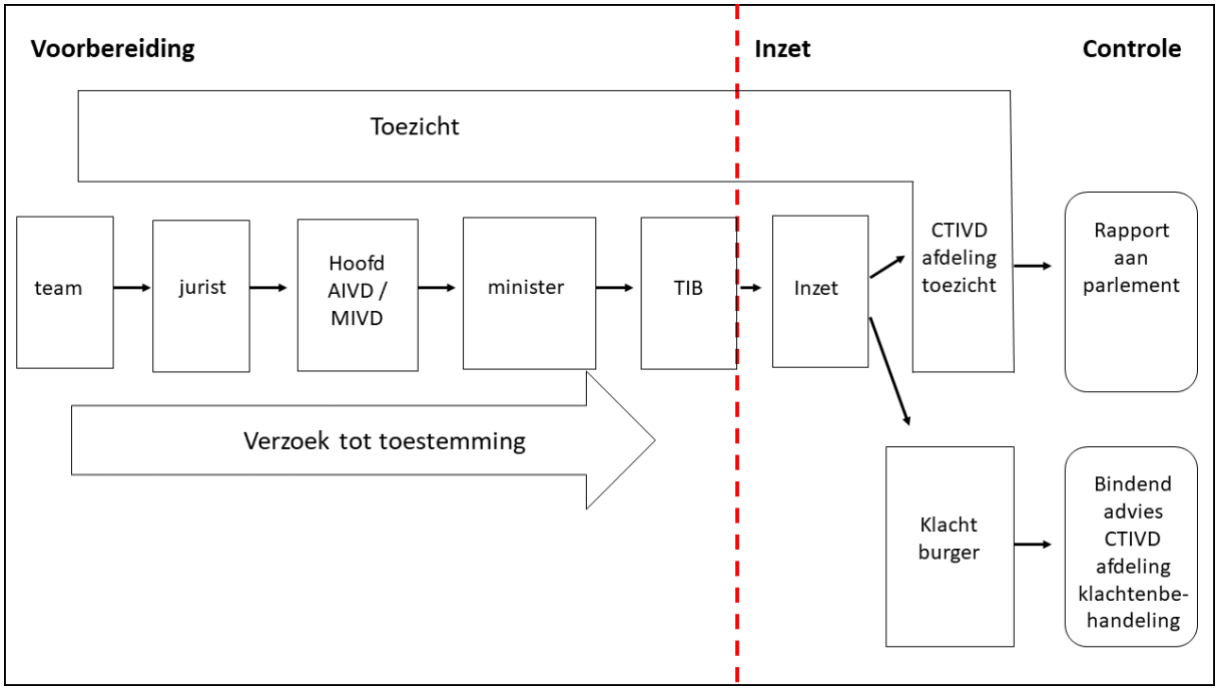
Mijn kritiek op de regeling voor metadata-analyse in artikel 50 Wiv 2017 richt zich op twee elementen: (1) een lastig uitvoerbare voorafgaande aanvraag en (2) de beperkte reikwijdte van de bijzondere bevoegdheid.

2.1. Uitvoerbaarheid van de aanvraag

Voor metadata-analyse uit bulkinterceptie is toestemming van de minister van BZK of Defensie vereist, voor zover de metadata-analyse is gericht op het identificeren van personen of organisaties.[17]

De aanvraag tot inzet van metadata-analyse uit bulkinterceptie ter identificatie van een persoon of organisatie (artikel 50 lid 1 sub b jo lid 4 Wiv 2017) doorloopt hetzelfde proces als andere aanvragen van bijzondere bevoegdheden. Een aanvraag tot inzet van de bijzondere bevoegdheid wordt geformuleerd vanuit de behoefte van een team van de AIVD of de MIVD en gaat (via de afdeling juridische zaken van de desbetreffende dienst en het hoofd van de dienst) naar de minister van BZK of Defensie. Deze geeft al dan niet toestemming voor de inzet van de bevoegdheid. Vervolgens voert de nieuwe opgerichte TIB haar rechtmatigheidstoets uit voor de meeste bijzondere bevoegdheden.[18] De CTIVD voert een rechtmatigheidstoets uit tijdens en na de inzet van alle bevoegdheden van de AIVD en de MIVD. In de memorie van toelichting wordt het toezichtstelsel als volgt weergegeven.

[14] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 111.
[15] Een 'target' is een persoon of organisatie waar de AIVD of de MIVD onderzoek naar verricht.
[16] CITVD-rapport nr. 38 (2014), p. 28.
[17] Artikel 50 lid 1 sub b jo lid 4 Wiv 2017.
[18] Met uitzondering van bepaalde vormen van observeren, de inzet van een 'agent', de verstrekking van gebruikers- en verkeersgegevens, en de toegang tot plaatsen. Voor het openen van brieven en de inzet van bijzondere bevoegdheden jegens advocaten en journalisten moet de rechtbank Den Haag toestemming geven. Zie artikel 32 lid 2 Wiv 2017.



Figuur 1: toezichtstelsel bij de inzet van bijzondere bevoegdheden op de AIVD en de MIVD[19]

De TIB toetst aan de wettelijke vereisten van de inzet van de bijzondere bevoegdheid en de algemene vereisten. De algemene vereisten bij de inzet van bijzondere bevoegdheden betreft een toets op de (1) noodzaak, (2) proportionaliteit en (3) subsidiariteit van de inzet van de bijzondere bevoegdheid.[20]

In de memorie van toelichting staat aangegeven dat in de praktijk de metadata wordt gecorreleerd met andere gegevensbestanden die de diensten ter beschikking hebben (artikel 50 lid 1 sub b jo lid 4 jo artikel 60 Wiv 2017).[21] In dat geval moet in de toestemming de betrokken gegevensbestanden worden aangeduid, omdat deze van belang is om aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit te toetsen.[22] Ten slotte moet de aanvraag een aanduiding bevatten van de gegevensbestanden die in de geautomatiseerde data-analyse worden betrokken.De toestemming kan worden verleend voor een periode van *twaalf* maanden en telkens op verzoek voor eenzelfde periode worden verlengd.

Naar aanleiding van het raadgevend referendum en ter uitvoering van de motie Recourt is in artikel 5 Beleidsregels Wiv 2017 het gerichtheidsvereiste als extra eis geformuleerd bij de inzet van bijzondere bevoegdheden.[23] Bij het verzoek om toestemming bij de inzet van een bijzondere bevoegdheid moet worden aangegeven op welke wijze de bijzondere bevoegdheid 'zo gericht mogelijk' wordt ingezet. Één jaar lang was er geen toelichting op dit nieuwe vereiste bij de inzet van bijzondere bevoegdheden, waardoor het onduidelijk was wat het gerichtheidsvereiste precies inhield. In de toelichting op het wetsvoorstel 'Wijzigingswet Wiv 2017' wordt het beschreven als 'een toets op in hoeverre bij de verwerving sprake is van het tot een minimum beperken van niet strikt voor het onderzoek noodzakelijke gegevens, gelet op de technische en operationele omstandigheden van de casus'. De te vergaren gegevens moeten daarbij worden afgebakend, bijvoorbeeld op basis van geografische gegevens, naar tijdstip, soort data en object.[24] Bovendien richt de toets zich klaarblijkelijk op de verwerving (de verzameling van gegevens). Het is

[19] Zie *Kamerstukken II* 2016/2017, 34588, nr. 3, p. 52.
[20] Zie artikel 26 en artikel 29 Wiv 2017.
[21] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 112.
[22] Idem. Zie ook artikel 26 en artikel 29 Wiv 2017.
[23] *Kamerstukken II* 2017/18, 34588, nr. 70.
[24] *Kamerstukken II* 2018/19, 35242, nr. 3, p. 4-5.

onduidelijk is hoe deze eis zich verhoudt tot de verdere verwerking van de gegevens, zoals bij metadata-analyse.

In de praktijk blijkt dat het voor de AIVD en de MIVD lastig is een goede aanvraag te formuleren voor de inzet van de bijzondere bevoegdheid van metadata-analyse uit bulkinterceptie.[25] In mei 2019 was in een toezichtsrapport van de CTIVD over de implementatie van de Wiv 2017 te lezen dat de inzet van de bijzondere bevoegdheid slechts was goedgekeurd voor force protection.

Het is mijns inziens ook niet zo gek dat het lastig is een aanvraag te formuleren voor de inzet van de bijzondere bevoegdheid, met name vanwege de aanduiding van de toe te passen verwerkingsvormen en de gegevensbestanden die in de analyse worden meegenomen. Het lijkt wel alsof de memorie van toelichting uitgaat van een situatie waar uitgeprinte vellen A4-papier met elkaar worden vergeleken en een handgeschreven verslag van de analyse wordt gemaakt, waarbij van te voren al duidelijk is welke gegevensbestanden bij analyse moeten worden betrokken. In de praktijk worden gegevens geautomatiseerd met elkaar vergeleken in verschillende databronnen (de 'naslag in geïntegreerde gegevensbronnen') of met behulp van applicaties bijvoorbeeld nagegaan wie met wie bellen (een netwerkanalyse). Daarnaast geeft de memorie van toelichting aan dat blijkbaar tot op zekere hoogte het verplaatsingsgedrag en het surfgedrag is van personen kan worden nagegaan. Dit zijn verschillende typen data-analyses die in een dynamisch proces plaatsvinden. Pas bij het uitvoeren van de analyses wordt duidelijk welke gegevensbestanden daarbij daadwerkelijk worden betrokken. De Wiv 2017 schrijft echter voor dat toestemming wordt gevraagd voor gedurende één jaar analyses uit te voeren ter identificatie van personen of organisaties, waarbij van te voren al duidelijk moet zijn welke vormen van analyses worden uitgevoerd, welke gegevensbestanden daarbij worden betrokken en waarom aan alle algemene vereisten bij de inzet van bijzondere bevoegdheden wordt voldaan.

Kortom, de voorwaarden voor de inzet van de bevoegdheid voor metadata-analyse zijn hetzelfde als bij de inzet van andere bijzondere bevoegdheden. Bijzondere bevoegdheden gaan doorgaans over het *verzamelen* van gegevens (met bijvoorbeeld een tap, de hackbevoegdheid, inzet van agenten, et cetera). Bij metadata-analyse gaat het echter om het *verwerken* van gegevens, terwijl de voorwaarden van de inzet hetzelfde blijven. Dat botst en maakt het zeer lastig – zo niet onmogelijk – een goede aanvraag te formuleren voor de inzet van de bijzondere bevoegdheid tot metadata-analyse uit gegevens van bulkinterceptie. Het is op voorhand niet goed in te schatten hoe het proces van data-analyse verloopt voor in de taakuitvoering in het kader van de nationale veiligheid van de diensten.

2.2. De beperkte reikwijdte van de bijzondere bevoegdheid

De inbreuk op persoonlijke levenssfeer is bij metadata-analyse op telecommunicatiegegevens uit bulkinterceptie net zo groot, als bij metadata-analyse op gegevens afkomstig uit *andere bevoegdheden* zijn verkregen dan bulkinterceptie. In rapport nr. 38 (2014) rapporteerde de CTIVD bijvoorbeeld dat ook grote hoeveelheden telecommunicatiegegevens zijn verkregen met de inzet van de hackbevoegdheid en de inzet van agenten.

De regeling is in artikel 50 lid 1 sub b Wiv 2017 te beperkt, omdat het alleen extra waarborgen biedt als gegevens zijn verkregen uit bulkinterceptie (artikel 48-49 Wiv 2017). Dat zijn feitelijk gegevens uit radioverkeer, satellietverkeer, telefonieverkeer en internetverkeer.[26] De AIVD en de MIVD verzamelen echter ook andere gegevens in grote hoeveelheden (bulk). CTIVD rapport nr. 71 (2020) gaat bijvoorbeeld over het verzamelen van passagiersgegevens van luchtvaartmaatschappijen in grote hoeveelheden. Deze 'bulkdataset' wordt bovendien gecombineerd met andere gegevens teneinde meer informatie over targets te weten te komen. De gegevens worden ook gebruikt om nieuwe targets te identificeren.

[25] CTIVD-rapport nr. 69 (2020) (Voortgangsrapportage IV Implementatie Wiv 2017) (augustus 2020).
[26] Zie CTIVD-rapport nr. 63 (2019) over de toepassing van filters bij OOG-interceptie door de AIVD en MIVD.

Vanuit het achterliggende idee van de bescherming van de rechten en vrijheden van burgers, is het vreemd dat de specifieke regeling tot metadata-analyse alleen geldt voor gegevens die zijn verkregen uit bulkinterceptie. Ook bij metadata-analyse uit andere bronnen van gegevens dan bulkinterceptie, zoals de hackbevoegdheid, is een specifieke regeling met waarborgen op zijn plaats.

Daarnaast is het vreemd dat de waarborg van toestemming van de minister en een oordeel van de TIB alleen geldt voor metadata-analyse 'ter identificatie van personen of organisaties' (art. 50 lid 4 Wiv 2017). Het in kaart brengen van het verplaatsingsgedrag of internetsurfgedrag van een target levert eveneens een ernstige privacy-inbreuk op. In de 'Privacy Impact Assessment' (PIA) op het wetsvoorstel van de Wiv 2017 wordt ook opgemerkt dat ook bij de verwerking van andersoortige gegevens dan telecommunicatiegegevens, zoals reisgegevens en financiële gegevens, een ernstige privacy-inbreuk kan plaatsvinden. Daar moeten voldoende waarborgen tegenover staan.[27]

Kortom, er is een discrepantie tussen de wettelijke waarborgen en privacybescherming bij metadata-analyse uit communicatiegegevens van bulkinterceptie en de wettelijke waarborgen bij data-analyse op andere databronnen.

3. Verwerking van gegevens door geautomatiseerde data-analyse

Metadata-analyse is slechts één vorm van geautomatiseerde data-analyse die de AIVD en de MIVD kunnen toepassen.[28] Bij geautomatiseerde data-analyse kan het ook gaan om (a) het op geautomatiseerde wijze onderling vergelijken van gegevens, (b) het doorzoeken van gegevens aan de hand van profielen ('profiling'), (c) het vergelijken van gegevens met het oog op het opsporen van bepaalde patronen ('machine learning').[29] Deze andere vormen van data-analyse kunnen ook een inbreuk op de grondrechten en fundamentele rechten van betrokkenen met zich meebrengen, terwijl hier geen bijzondere bevoegdheid voor geregeld is, zoals bij metadata-analyse uit bulkinterceptie.[30]

Geautomatiseerde data-analyse zijn gegevensverwerkingen die worden genormeerd door de algemene bepalingen omtrent gegevensverwerking en de speciale regeling in artikel 60 Wiv 2017. Deze bepalingen worden in deze paragraaf kort beschreven. Ook wordt nader ingegaan op de nieuwe bepaling over de zorgplicht omtrent gegevensverwerking en de toepassing daarvan bij de verwerking van gegevens uit bulkdatasets. In deze paragraaf wordt ook de recente jurisprudentie van het EHRM en HvJ EU over metadata-analyse geanalyseerd.

3.1. Algemene bepalingen omtrent gegevensverwerking

Het begrip 'gegevensverwerking' omvat kort gezegd elke handeling of elk geheel van handelingen met betrekking tot gegevens.[31] Vergeleken met andere wetgeving omtrent de verwerking van persoonsgegevens is hierbij opvallend dat de Wiv 2017 de algemene bepalingen omtrent gegevensverwerking toepast op álle verwerkingen van gegevens en niet alleen betrekking heeft op de verwerking van persoonsgegevens.

De algemene bepalingen omtrent gegevensverwerking zijn in de loop der jaren niet ingrijpend gewijzigd. Al in de Wiv 1987 is bijvoorbeeld te lezen dat gegevensverwerking slechts mag plaatsvinden met een bepaald doel (het beginsel van doelbinding) en slechts voor zover dat

[27] Zie B.J. Koops e.a., 'Privacy Impact Assessment Wet op de inlichtingen-en veiligheidsdiensten 20XX', TNO/TILT 2016, p. 63.
[28] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 112.
[29] Zie artikel 60 Wiv 2017.
[30] Zie voor een overzicht bijvoorbeeld M. Vetzo, & J.H. Gerards, 'Algoritme-gedreven technologieën en grondrechten', *Computerrecht* 2019/3, p. 10-19.
[31] Artikel 1 sub f Wiv 2017.

noodzakelijk is voor de taakuitvoering (het noodzakelijkheidsbeginsel). De doelen van de gegevensverwerking staan genoemd in artikel 19 lid 1 en lid 2 Wiv 2017, zoals de verwerking van gegevens van degenen van wie wordt vermoed dat zij een gevaar vormen voor de nationale veiligheid en de verwerking van gegevens van personen die toestemming hebben verleend voor een veiligheidsonderzoek door de AIVD of de MIVD.[32]

De Wiv 2017 schrijft in artikel 18 voor dat de gegevensverwerking op 'behoorlijke en zorgvuldige wijze' moet plaatsvinden. Dit betekent ook dat de gegevensverwerking evenredig moet zijn ten opzichte van het doel van de verwerking (proportionaliteitsbeginsel).[33] Voor de verwerking van gevoelige gegevens bestaan ook extra waarborgen. Gevoelige gegevens zijn in artikel 19 Wiv 2017 gedefinieerd als 'persoonsgegevens omtrent iemands godsdienst of levensovertuiging, ras, lidmaatschap van een vakvereniging, gezondheid en seksuele leven'. Deze gegevens mogen slechts worden verwerkt als dat 'onvermijdelijk' is voor de taakuitvoering. Met het begrip 'onvermijdelijk' wordt beoogd aan te geven dat bij de verwerking van een gegeven als hier bedoeld aan een zwaarder criterium dient te worden voldaan dan aan het noodzakelijkheidscriterium in artikel 18 lid 1 Wiv 2017.[34] Over de invulling van het criterium in de praktijk is verder niet veel bekend.

De bijzondere bepaling voor geautomatiseerde data-analyse in artikel 60 Wiv 2017 is deels ingegeven uit zorgen over 'big data analyses' en technieken als 'profiling'. Het WRR-rapport over 'Big data' in 2016 is daarbij een katalysator geweest voor artikel 60 Wiv 2017.[35] In het WRR-rapport over data-analyse rapporteert het adviesorgaan dat de gegevens voor analyses door veiligheidsinstanties, zoals de AIVD en de MIVD, veelal afkomstig zijn uit overheidsbronnen. Daarbij moet worden gedacht aan financiële gegevens en registratiegegevens, vrij opvraagbare openbare bronnen en gegevens uit sociale media.[36]

In de memorie van toelichting van de Wiv 2017 gaat de wetgever in op de risico's van gegevensverwerking en wordt verwoord hoe het gebruik van profielen die op basis van big data en algoritmen zijn gegenereerd kan leiden tot 'bias' in datasets en kan leiden tot uitkomsten die stelselmatig bepaalde groepen bevoor- of benadelen.[37] Dit vormt de achtergrond van het verbod op geautomatiseerde besluitvorming in artikel 60 lid 3 Wiv 2017.[38] Hoewel er niet naar verwezen wordt, is het verbod op geautomatiseerde besluitvorming vergelijkbaar met de regeling in de AVG[39] en in de richtlijn gegevensbescherming opsporing en vervolging[40].

Toch is het verbod op het nemen van maatregelen 'uitsluitend op basis van de resultaten van een geautomatiseerde data-analyse' ongelukkig geformuleerd. De term 'maatregelen' wordt namelijk niet toegelicht in de wetsgeschiedenis. Bekend is dat de AIVD en de MIVD maatregelen mogen nemen in het kader van de nationale veiligheid om bijvoorbeeld (de voorbereiding van) een aanslag door terroristen te verstoren.[41] Het ligt echter voor de hand dat de term breder moet worden uitgelegd en bijvoorbeeld ook uitstrekt tot het nemen van een besluit over het verstrekken van een 'verklaring omtrent gedrag' door de AIVD en de MIVD in veiligheidsonderzoeken. Dat sluit aan bij richtlijn gegevensbescherming opsporing en vervolging waarin staat dat het verbod geldt bij gegevensverwerkingen die 'voor de betrokkene nadelige rechtsgevolgen heeft of hem in aanmerkelijke mate treft'.

[32] De taken van de AIVD en de MIVD staan opgesomd in artikel 8 en 10 Wiv 2017.
[33] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 32.
[34] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 34.
[35] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 131.
[36] WRR-rapport nr. 95, 'Big Data in een vrije en veilige samenleving', Den Haag: Amsterdam University Press 2016, p. 66-67 (hierna: WRR-rapport nr. 95 (2016)).
[37] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 131.
[38] Artikel 60 lid 3 Wiv 2017: *"Het bevorderen of treffen van maatregelen jegens een persoon uitsluitend op basis van de resultaten van een gegevensverwerking als bedoeld in het tweede lid is niet toegestaan"*
[39] Zie artikel 22 van de Algemene Verordening Gegevensbescherming.
[40] Zie artikel 11 van de EU richtlijn 2016/680.
[41] De term komt voor in artikel 73 Wiv 2017.

De CTIVD heeft in aansluiting de term eerder uitgelegd als het verbod 'dat (operationele) besluiten en handelingen die (substantiële) gevolgen hebben voor personen of groepen personen niet uitsluitend gebaseerd mogen worden op de uitkomst van geautomatiseerde data-analyse, zonder dat die uitkomst eerst door een mens is beoordeeld'.[42] Het verdient aanbeveling dat de wetgever beter toelicht wat onder 'maatregelen' bij het verbod op geautomatiseerde besluitvorming moet worden verstaan.

3.2. Zorgplicht

De hoofden van de AIVD en de MIVD moeten de nodige technische, personele en organisatorische maatregelen nemen om voor zorg te dragen dat de verwerking van gegevens in overeenstemming met de Wiv 2017 plaatsvindt.[43] Deze maatregelen omvatten in ieder geval het 'treffen van voorzieningen ter bevordering van de juistheid en de volledigheid van de gegevens die worden verwerkt alsmede ter bevordering van de kwaliteit van de gegevensverwerking, waaronder begrepen de daarbij gehanteerde algoritmen en modellen' (artikel 24 Wiv 2017).

Meer specifiek zegt de wetgever over geautomatiseerde data-analyse dat bij nieuwe applicaties voor gegevensverwerking rekening wordt gehouden met 'privacy by design' en 'privacy by default'. Daarbij wordt 'gegevensbescherming by design' opgevat als een verplichting dat 'de diensten bij de ontwikkeling van systemen het belang van privacy en gegevensbescherming inbouwen'. 'Gegevensbescherming by default' ziet volgens de wetgever erop dat systemen 'zo ontworpen en ingericht worden dat zo min mogelijk persoonsgegevens worden verwerkt'.[44]

De zorgplicht houdt volgens de CTIVD ook in dat de AIVD en de MIVD zelf voortdurende controle uitoefenen op de wijze waarop zij gegevens verwerken. Zij moeten ervoor zorgen dat zij voldoen aan de wet (compliance) en dat blijven doen. Hiervoor moeten zij instrumenten (zoals interne controlemechanismen, dashboards en metrics) gebruiken die hen zicht geven op de werking van processen en systemen van gegevensverwerking en hen daardoor in staat stellen risico's te signaleren en tijdig maatregelen te nemen.[45]

De AIVD en de MIVD moeten nog grote stappen maken om daadwerkelijk en voldoende invulling te geven aan de zorgplicht bij geautomatiseerde data-analyse. Uit de vierde voortgangsrapportage (augustus 2020) over de implementatie van de Wiv 2017 bleek dat de diensten nog een 'vertaalslag moeten maken van wet en beleid naar de uitvoeringspraktijk'.[46] De diensten hebben wel een impactanalyse voor hun organisaties opgesteld en een *Joint Data Compliance Team* (JDCT) in de *Joint Sigint Cyber Unit* (JSCU) opgericht, maar er is volgens de CTIVD nog weinig invullingen gegeven aan de algemene bepalingen die zien op een zorgvuldige gegevensverwerking (art. 18-24 Wiv 2017) voor de werkvloer.

3.3. Tijdelijke regeling verdere verwerking bulkdatasets

Een voorbeeld van specifieke regeling voor geautomatiseerde data-analyse die ondertussen wel tot stand is gekomen, is de 'Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017' die op 5 november 2020 is gepubliceerd.[47] Een bulkdataset is een omvangrijke gegevensverzameling waarbij het merendeel van de gegevens betrekking heeft op personen en/of organisaties die geen onderwerp van onderzoek zijn van een dienst en dat ook niet worden. Deze regeling voor bulkdatasets is een reactie op CTIVD-rapport nr. 70 over bulkdatasets door inzet van de hackbevoegdheid en rapport nr. 71 over het verzamelen van passagiersgegevens door inzet van de

[42] CTIVD-rapport nr. 62 (2019).
[43] De bepaling is opgenomen naar aanleiding van een aanbeveling uit de 'Privacy impact assessment Wiv 20XX' en de inbreng van de CTIVD in de zienswijze op de wet in 2016, alsmede naar aanleiding van het daaropvolgende parlementaire debat (*Kamerstukken II* 2016/17, 34588, nr. 18, p. 8).
[44] *Kamerstukken II* 2016/17, 34588, nr. 18, p. 22.
[45] De vier voortgangsrapportages van de CTIVD over de implementatie van de Wiv 2017 geven onder meer zicht op het proces van de implementatie van de zorgplicht op de gegevensverwerking bij de diensten.
[46] CTIVD-rapport nr. 69 (2020), p. 17.
[47] *Stcrt*. 2020, 56482.

informantenbevoegdheid. Hieronder wordt nader ingegaan op de twee belangrijkste waarborgen uit de regeling: de beperking van toegang tot gegevens en de periodieke (her)beoordeling van de noodzaak het bewaren van de bulkdataset.[48]

De toegang van AIVD- en MIVD-medewerkers wordt beperkt afhankelijk van de ernst van inmenging op de persoonlijke levenssfeer van personen die plaatsvindt bij de verwerking van de gegevens in de bulkdataset. De ernst van de inmenging wordt bepaald op basis van de volgende vier elementen: (1) identificerende gegevens, (2) locaties, (3) netwerk van de contacten van een persoon en (4) vertrouwelijke inhoud. Hierbij valt op dat de verwerkingsvormen van de gegevens uit de bulkdatasets niet worden meegenomen om de privacy-inbreuk te bepalen, terwijl dit volgens EHRM wel een belangrijke factor is om de ernst van de privacy-inmenging te bepalen.[49]

De toegang tot bulkdatasets is ingedeeld in een (a) standaard toegangsregime, (b) beperkt toegangsregime of (c) strikt beperkt toegangsregime. Onder het standaard toestemmingregime behoren medewerkers die toegang vanuit hun functie nodig hebben, zoals medewerkers die het inlichtingenonderzoek uitvoeren maar ook data-analisten en data-scientists. Onder het beperkt toegangsregime behoren functiegroepen die vanwege hun specifieke kennis en expertise met bulkdata de verbanden tussen verschillende gegevensbestanden inzichtelijk kunnen maken door middel van (geautomatiseerde) data-analyses. Dat kunnen medewerkers uit een inlichtingenteam zijn of een team dat belast is met de uitvoering van veiligheidsonderzoeken of het opstellen van dreigingsanalyses. Onder het strikte toegangsregime hebben alleen specifieke medewerkers met een bepaalde functie toegang of toegang waarbij de functionaliteit beperkt is tot het bevragen van gegevens. Een speciaal verzoek tot toestemming moet worden ingediend om toegang te krijgen tot gegevens in de bulkdataset als blijkt dat daarin zich een kenmerk bevindt, zoals een telefoonnummer.[50] De periodieke beoordeling vindt plaats om de drie jaar, twee jaar, of één jaar; afhankelijk van het type bulkdataset. Dan wordt beoordeeld of de dataset moet worden verwijderd.

In de regeling valt op dat de bulkdatasets geen maximale bewaartermijn kennen (de zojuist bovengenoemde beoordeling op betekenis kan worden herhaald) en de bulkdatasets kunnen in de tussentijd blijven groeien. Ondanks deze kritiekpunten kan de regeling worden gezien als een significante verbetering ten opzichte van de oude situatie en als een voorbeeld van de invulling de algemene bepalingen omtrent gegevensverwerking en de zorgplicht omtrent gegevensverwerking uit de Wiv 2017.

3.4. Jurisprudentie met betrekking tot data-analyse

De ernst van de privacy-inbreuk bij metadata-analyse en de noodzaak tot een nieuwe regeling is in de loop der jaren duidelijk geworden vanwege rapporten van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (hierna: CTIVD), het advies van de evaluatiecommissie Wiv 2002 (de Commissie-Dessens) en jurisprudentie van het EHRM.[51]

Uit jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) in (o.a.) de zaken *Liberty e.a. t. het Verenigd Koninkrijk*[52], *Brother Watch e.a*[53] met betrekking tot bulkinterceptie) en het Hof van Justitie van de Europese Unie (HvJ EU) in de zaken *Digital Rights*[54], *Tele2 Sverige en*

[48] In dit artikel wordt niet ingegaan op regeling voor de verstrekking van bulkdatasets aan een buitenlandse inlichtingen- en veiligheidsdienst.
[49] Zie, o.a., EHRM 2 september 2010, nr. 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305, par. 45 *(Uzun t. Duitsland*).
[50] Zie de toelichting op de tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017.
[51] Commissie-Dessens, *Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, 2013. Zie met name ook CTIVD-rapport nr. 38 (2014) over en de beleidsreactie daarop.
[52] EHRM 1 juli 2008, nr. 58243/00, ECLI:CE:ECHR:2008:0701JUD005824300, par. 69 (*Liberty e.a. t. het Verenigd Koninkrijk*).
[53] EHRM 13 september 2018, nrs. 58170/13, 62322/14, 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013, par. 356-357 (*Big Brother Watch e.a.t. het Verenigd Koninkrijk*) (sinds februari 2019 aanhangig bij de Grote Kamer).
[54] HvJ EU 8 april 2014, C-293/12 and C-594/12, ECLI:EU:C:2014:238, par. 27 (*Digital Rights t. Ierland*).

AB/Watson[55]*, Privacy International*[56]*,* en de samengevoegde zaken van *La Quadrature du Net e.a.*[57] met betrekking tot (bulk)dataretentie), volgt dat metadata-analyse, waarmee de contacten, bewegingen, internetgeschiedenis en communicatiepatronen van personen in kaart kunnen worden gebracht, een zwaarwegende inmenging in het recht op privacy inhoudt.

Tegenover deze ernstige privacy-inmenging moeten voldoende waarborgen tegenover staan om misbruik van overheidsmacht te voorkomen. In de zaak *Big Brother Watch* is het Verenigd Koninkrijk bijvoorbeeld veroordeeld voor een schending van artikel 8 EVRM bij de toepassing van bulkinterceptie (ook wel 'signals intelligence' (SIGINT) genoemd) door hun inlichtingen- en veiligheidsdiensten, mede vanwege het ontbreken van effectieve waarborgen met betrekking tot de analyse van de metadata van geïntercepteerde communicatie.[58]

De ernstige privacy-inbreuk die bij metadata-analyse plaatsvindt wordt door de Nederlandse wetgever in de memorie van toelichting in de Wiv 2017 erkend en vormt de ratio voor de introductie van de bijzondere bevoegdheid.[59] In de *Big Brother Watch-zaak* lijkt het EHRM wel ruimte te bieden voor een regeling zonder voorafgaande toestemming voor de verwerking van de gegevens. In dat geval moet naar het gehele systeem worden gekeken met alle 'checks and balances' die misbruik van de bevoegdheden moeten tegengaan.[60] Als 'check and balance' verdient het overweging de CTIVD een bindend oordeel in haar toezichtswerkzaamheden te geven en daarmee een interventiebevoegdheid te geven bij geconstateerde onrechtmatige gegevensverwerkingen.[61] In dat geval zou de toezichthouder bijvoorbeeld de opdracht kunnen geven gegevens te vernietigen als uit onderzoek blijkt dat gegevens onrechtmatig zijn verwerkt. Dit kan echter wel de informatiepositie van inlichtingen- en veiligheidsdiensten aantasten. In hun beleidsreactie op de rapporten over bulkdatasets en het advies van de CTIVD enkele bulkdatasets te vernietigen beargumenteren de ministers dat deze bulkdatasets noodzakelijk zijn voor onderzoeken van de diensten, met name om de 'onbekende dreiging' voor de nationale veiligheid in de toekomst te onderkennen. In de beleidsreactie lichtten de ministers toe dat de gegevens in bulkdatasets onder andere van essentieel belang waren bij het onderkennen van locaties van Nederlandse uitreizigers in (voormalig) ISIS-gebied, in onderzoek naar de inzet van 'Improvised Explosive Devices' (IED's) tegen Nederlandse militairen, in het onderzoek naar de betrokkenheid van de Iraanse dienst bij liquidaties in Nederland en voor het vaststellen van de identiteit van personen die betrokken zijn bij zenuwgasaanvallen in Syrië in 2016/2017.[62] Als tegenwicht kan hier op overwogen worden een beroepsmogelijkheid in te bouwen, zodat uiteindelijk een rechterlijke instantie daarover een beslissing neemt.

In de zeer recente zaken van *La Quadrature du Net e.a.*.[63] komt het Hof van Justitie tot de conclusie dat zij zich ook kunnen uitspreken over de verwerking van (bulk)gegevens door inlichtingen- en veiligheidsdiensten die worden bewaard in het kader van dataretentie.[64] Deze vergaande beslissing vereist eigenlijk meer toelichting, gezien het feit dat nationale veiligheid tot de exclusieve competentie van Lidstaten wordt gerekend in het Verdrag tot de oprichting van de

[55] HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:572 en ECLI:EU:C:2016:970, par. 99 (*Tele2 Sverige AB en Watson*).
[56] HvJ EU 6 oktober 2020, C-623-17, ECLI:EU:C:2020:790, par. 70-73 (*Privacy International* t. *Verenigd Koninkrijk*).
[57] HvJ EU 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, par. 117, 153 en 174 (*La Quadrature du Net e.a*. t. *Frankrijk)*
[58] *Big Brother Watch e.a.*, par. 346-347 en 357.
[59] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 111.
[60] *Big Brother Watch e.a.,* par. 320.
[61] De CTIVD kent op dit moment alleen de mogelijkheid tot een bindend oordeel bij klachten. Zie over bindend toezicht ook artikel 15 en artikel 19 van het Protocol tot wijziging van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens van 10 oktober 2018, Straatsburg, *Trb.* 2018, 201 (Verdrag 108+). Zie *La Quadrature du Net e.a*. t. *Frankrijk*, par. 139 en 179.
[62] Kamerbrief van 22 september 2020 (Beleidsreactie CTIVD onderzoeken passagiersgegevens en verwerving bulkdata door bevoegdheid tot binnendringen).
[63] HvJ EU 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net e.a*. t. *Frankrijk*).
[64] *La Quadrature du Net*, par. 99-104.

Europese Unie.[65] Het HvJ EU acht een vorm van dataretentie van telecommunicatiegegevens (in essentie ook een bulkdataset) mogelijk, voor zover staten voor een 'serieuze bedreiging voor de nationale veiligheid' staan die 'oprecht', 'actueel' en 'voorzienbaar' is.[66] Het is nog onduidelijk wat de consequenties van deze uitspraak zijn voor de praktijk bij het verzamelen van bulkdatasets.

Metadata-analyse op telecommunicatiegegevens wordt door het HvJ EU gezien als een ernstige privacy-inbreuk, waarbij onafhankelijk toezicht op de gegevensverwerking bindend moet zijn, de metadata-analyse niet slechts mag plaatsvinden op basis van gevoelige gegevens en benadrukt het verbod op geautomatiseerde besluitvorming zonder menselijke toets.[67] Afgezien van het ontbreken van een bindend element bij gegevensverwerking, lijkt de Wiv 2017 verder geen aanpassing te behoeven.

4. Oplossingsrichting 1: een nieuwe bevoegdheid voor metadata-analyse

Een oplossing voor de geschetste problematiek in paragraaf 2.1 over de slechte uitvoerbaarheid van de aanvraag van de bijzondere bevoegdheid is mogelijk deels gelegen in het koppelen van de bijzondere bevoegdheden van 'selectie' en metadata-analyse. Selectie is het kennisnemen van inhoudelijke gegevens uit bulkinterceptie.[68] In de praktijk vindt selectie plaats met behulp van selectiecriteria. Selectiecriteria zijn bijvoorbeeld telefoonnummers of e-mailadressen die bij een target horen. Het kunnen ook trefwoorden zijn die aan een nader omschreven persoon, organisatie of onderwerp zijn gerelateerd waar de AIVD of de MIVD onderzoek naar doen. In de aanvraag voor de inzet van de selectiebevoegdheid worden de personen, organisaties en onderwerpen omschreven waar de bevoegdheid zich op richt. Voor het koppelen van de selectiecriteria aan een persoon, organisatie of onderwerp is intern toestemming vereist. De selectiecriteria die horen bij de in de aanvraag beschreven personen, organisaties of onderwerpen hoeven niet aan de minister en de TIB te worden voorgelegd.[69]

Als toestemming voor de inzet van de bijzondere bevoegdheid tot selectie is verkregen, worden de gegevens aan de hand van selectiecriteria geselecteerd uit de onderschepte communicatie, zoals telefonieverkeer, satellietverkeer en internetverkeer. Het selecteren van dit verkeer veronderstelt dat onderscheid kan worden gemaakt tussen metadata en inhoud. Immers, de bijzondere bevoegdheid richt zich op het selecteren van de *inhoud* van het verkeer. De Wiv 2017 bevat echter geen definitie van 'metadata'. Meer algemeen kunnen metagegevens worden beschreven als gegevens 'over de gegevens', die niet de inhoud van communicatie betreffen. De inhoud van communicatie betreft bijvoorbeeld de inhoud van een telefoongesprek of de inhoud van een elektronisch verstuurd bericht. In artikel 4 van het Besluit gegevensverstrekking onderzoek van communicatie Wiv 2017 wordt metadata meer technisch beschreven als gegevens zoals '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'.[70] Het blijkt in de praktijk lastig onderscheid te maken tussen inhoud en metadata bij internetverkeer.[71] Het is bijvoorbeeld onduidelijk of de URL naar een website als inhoud of metadata moet worden gezien.[72]

[65] Artikel 4 lid 2 van het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie. Zie ook Plixavra Vogiatzoglou en Jenny Bergholm, 'Privacy International & La Quadrature du Net: the latest on data retention in the name of national and public security', *blog KU Leuven*, oktober 2020.
[66] Vertaald uit de woorden 'genuine', 'present' en 'forseeable' (*La Quadrature du Net*, par. 137).
[67] Zie *La Quadrature du Net*, par. 179-182.
[68] Artikel 50 lid 1 sub a Wiv 2017.
[69] Zie uitgebreid CTIVD-rapport nr. 64 (2019) over de inzet van de bijzondere bevoegdheid tot selectie door de AIVD en de MIVD.
[70] *Stb.* 2017, 116. Zie ook *Kamerstukken II* 2016/17, 34588, 3, p. 111.
[71] Zie uitgebreid E.J. Koops & J.M. Smits, *Verkeersgegevens en artikel 13 Grondwet. Een technische en juridische analyse van het onderscheid tussen verkeersgegevens en inhoud van communicatie*. Wolf Legal Publishers (WLP) 2014.
[72] CTIVD-rapport nr. 64 (2019), p. 13.

De oplossingsrichting zit in het idee de bijzondere bevoegdheid voor metadata-analyse te combineren met de bijzondere bevoegdheid voor selectie, zodat na toestemming voor selectie ook metadata-analyse mag plaatsvinden. Het problematische onderscheid tussen metadata en inhoud speelt dan geen rol meer. De nadruk ligt ook niet meer op een voorafgaande toets op de vormen van data-analyse zelf, maar op de personen en organisaties in relatie tot de onderzoeken. Met de bijzondere bevoegdheid tot 'search gericht op selectie' in artikel 49 lid 2 Wiv 2017 is het ook mogelijk door (speciaal geautoriseerde medewerkers) metadata-analyse uit te voeren op het gehele onderschepte verkeer om nieuwe targets (personen of organisaties) te onderkennen. Met deze oplossing is er meer ruimte voor een dynamisch proces van data-analyse en kan worden aangesloten bij een bestaande en goed werkende bevoegdheid bij bulkinterceptie. Daarbij wordt dus tegemoetgekomen aan een beter werkbaar systeem voor metadata-analyse.

Het lost echter niet het probleem op dat de bijzondere bescherming (in de vorm van een speciale regeling met waarborgen), alleen bestaat voor gegevens uit bulkinterceptie en niet voor metadata-analyse bij gegevens die afkomstig zijn uit andere bijzondere bevoegdheden of data-analyses die worden uitgevoerd op andere typen gegevens dan telecommunicatiegegevens. Eerder is aangegeven dat metadata-analyse ook plaatsvindt uit andere bronnen van (bulk)data die zijn verkregen met andere bevoegdheden, zoals de hackbevoegdheid. In mijn oratie heb ik betoogd dat het wenselijk is een bulkbevoegdheid te creëren voor het verzamelen van bulkdatasets.[73] Stel dat een bulkbevoegdheid wordt gecreëerd is het een mogelijkheid in aansluiting met een bredere selectiebevoegdheid bij bulkinterceptie, ook een bevoegdheid te creëren voor het kennisnemen van gegevens uit andere bulkdatasets.

5. Oplossingsrichting 2: specifieke regels als uitwerking zorgplicht

De tweede oplossing voor de problematiek in paragraaf 2.2 over de beperkte reikwijdte van de huidige bijzondere bevoegdheid is om de bijzondere bevoegdheid tot metadata-analyse in artikel 50 lid 1 sub b Wiv 2017 te schrappen en nadrukkelijk invulling te geven aan de algemene bepalingen voor gegevensverwerking als een ernstige inmenging met het recht op privacy en het recht op de bescherming van persoonsgegevens plaatsvindt.

Vanuit de zorgplicht in artikel 24 Wiv 2017 moet het hoofd van de AIVD en de MIVD technische, personele en organisatorische maatregelen nemen in verband met de verwerking van gegevens. Daarbij moet op grond van artikel 24 lid 2 sub b Wiv 2017 aandacht zijn voor de gehanteerde algoritmen en modellen en kunnen op grond artikel 24 lid 2 sub c Wiv 2017 personen worden aangewezen die bij uitsluiting van anderen bevoegd zijn de gegevens te verwerken.[74]

Als wordt gekozen metadata-analyse als een algemene bevoegdheid te behandelen, dan kunnen de AIVD en de MIVD dat in theorie voor iedere taak uitvoeren, zoals veiligheidsonderzoeken die worden uitgevoerd om te bepalen of een persoon een zogenoemde 'vertrouwensfunctie' mag bekleden.[75] Bijzondere bevoegdheden mogen alleen worden ingezet voor bepaalde taken, zoals onderzoeken naar de targets en organisaties die de nationale veiligheid bedreigen en voor het verwerken van gegevens voor de inlichtingentaak buitenland.[76] De diensten zouden ook per dataset kunnen bepalen voor welke taken de gegevens mogen worden verwerkt. In de regeling voor de verwerking van gegevens uit bulkdatasets (zoals besproken in paragraaf 3.3) is de verwerking van gegevens in bulkdatasets mogelijk voor alle taken, waaronder de taakuitvoering ten behoeve van veiligheidsonderzoeken door de AIVD en de MIVD.

[73] Zie J.J. Oerlemans, 'Grenzen stellen aan datahonger. De bescherming van de nationale veiligheid in een democratische rechtsstaat', inaugurele rede, Universiteit Utrecht 2020.
[74] Zie paragraaf 3.2.
[75] De taken van de AIVD en de MIVD worden in artikel 8 en artikel 10 Wiv 2017 benoemd.
[76] Artikel 28 Wiv 2017. De zogenoemde a- en d-taak staan in artikel 8 Wiv 2017 (voor de AIVD).

Voor gegevensverwerkingen die een ernstige inbreuk op het recht op privacy en het recht op bescherming van gegevens kunnen maken, dienen specifieke maatregelen te worden genomen als waarborg. Daarbij kan gedacht worden aan een strikt autorisatieregime, zodat alleen werknemers met bepaalde functies waarvoor de toegang noodzakelijk is, toegang krijgen. Ook kan worden gedifferentieerd in de functionaliteiten van applicaties in combinatie met autorisaties die worden gebruikt voor de verwerking van gegevens. Ook moet over de omgang van gegevens worden nagedacht, zoals de opslag van tussentijdse of tijdelijke resultaten van data-analyse en het stellen van bewaartermijnen. Telkens is ook een maatregel zoals interne logging bij het gebruik van applicaties en de (ook interne) controle daarop noodzakelijk.

De tweede oplossingsrichting heeft als nadeel dat er geen onafhankelijk toezichthouder van te voren toestemming geeft voor de gegevensverwerkingen die een ernstige privacy-inmenging met zich meebrengen. Tijdens de gegevensverwerking en achteraf heeft de CTIVD geen bindend toezicht, waardoor niet kan worden overgegaan tot het stopzetten of het vernietigen van gegevens als deze door de diensten onrechtmatig zijn verwerkt. Dit lijkt niet te voldoen aan de vereisten van het HvJ EU in de meest recente over dataretentie.[77] De wetgever moet ook in het kader van 'checks and balances' en de implementatie van Verdrag 108+ nagaan of het huidige toezichtstelsel met beperkte interventiemogelijkheid bij de verwerking van gegevens voldoende is.[78]

6. Conclusie

De Wiv 2017 normeert metadata-analyse uit bulkinterceptie een stuk strenger dan de Wiv 2002. Als gevolg van de Snowden-onthullingen, aanbevelingen van de toezichthouder en Commissie-Dessens, en jurisprudentie van het EHRM, is een bijzondere bevoegdheid gecreëerd voor metadata-analyse van gegevens uit bulkinterceptie in artikel 50 van de Wiv 2017.

Het probleem is dat metadata-analyse uit bulkinterceptie nog zeer beperkt wordt toegepast, omdat het in de praktijk zeer lastig blijkt een aanvraag te formuleren voor de inzet van bijzondere bevoegdheid. Op voorhand is het bijzonder lastig aan te geven welke vormen van gegevens verwerking zullen plaatsvinden, welke bestanden daarbij worden betrokken en waarom dat proportioneel en "zo gericht mogelijk" is. Daarnaast is de regeling voor metadata-analyse in de Wiv 2017 te beperkt. Ook bij metadata-analyse uit andere bronnen van gegevens die worden verzameld na de inzet van bevoegdheden, zoals de hackbevoegdheid, doet zich een vergelijkbare privacy-inbreuk voor. Daarnaast kan zich bij andere verwerkingen van andere persoonsgegevens dan telecommunicatiegegevens ook een ernstige inbreuk op de persoonlijke levenssfeer voordoen die specifieke waarborgen rechtvaardigt.

Het onderliggende idee is het recht op privacy beter te bescherming door een specifieke regeling te treffen voor gegevensverwerkingen die een ernstige inbreuk op de persoonlijke levenssfeer van personen maken. Door in de wet een specifieke regeling op te nemen, kan misbruik van overheidsmacht worden tegengegaan. In dit preadvies worden twee oplossingsrichtingen gepresenteerd die de huidige regeling kunnen verbeteren, maar ook hun eigen nadelen kennen.

In de eerste oplossingsrichting zou de bevoegdheid tot selectie en metadata-analyse worden gecombineerd. Als toestemming is verleend tot het kennisnemen van gegevens uit bulkinterceptie op het niveau van personen, organisatie of trefwoorden, dan is het ook toegestaan daarop metadata-analyse toe te passen. Het is in dat geval niet noodzakelijk de verwerkingsvormen en de te betrekken gegevensbestanden van te voren in de aanvraag mee te nemen. Speciaal geautoriseerde medewerkers mogen in dat geval ook metadata-analyses uitvoeren om onbekende targets te identificeren. Als een meer algemene bulkbevoegdheid als bijzondere bevoegdheid wordt gecreëerd, kan deze meer algemene selectiebevoegdheid ook daarvoor worden geregeld, zodat de

[77] Zie over bindend toezicht *La Quadrature du Net e.a*. t. *Frankrijk*, par. 179.
[78] Zie artikel 15 en artikel 19 van het Protocol tot wijziging van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens van 10 oktober 2018, Straatsburg, *Trb.* 2018, 201 (Verdrag 108+).

waarborgen ook gelden als de gegevensverwerking plaatsvindt op andere databronnen dan gegevens uit bulkinterceptie.

In de tweede oplossingsrichting wordt voorgesteld de bijzondere bevoegdheid voor metadata-analyse te schrappen en een specifieke regeling te treffen voor de verwerking van persoonsgegevens bij metadata-analyse. Dat kan worden gezien als een uitvoering van de zorgplicht ten behoeve van een zorgvuldige gegevensverwerking, zoals in november 2020 is gedaan in de 'Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017'. Het is de vraag of deze nieuwe regeling voldoet aan de vereisten die door het EHRM en het HvJ EU worden gesteld bij de verwerking van gegevens uit bulkdatasets, zoals bij bulkinterceptie en bij dataretentie van telecommunicatiegegevens. Als extra waarborg kan overwogen worden de CTIVD een bindend oordeel te geven als uit onderzoek blijkt dat gegevens onrechtmatig (in strijd met de Wiv 2017) zijn verwerkt. Daarbij bestaan ook zorgen over de aantasting van de informatiepositie door een dergelijke maatregel.

Ten slotte doen zich andere risico's voor bij 'geautomatiseerde besluitvorming' na data-analyses op gegevensverwerking. Het verbod op geautomatiseerde besluitvorming zonder menselijke tussenkomst definieert niet goed wanneer het verbod van toepassing is. Aanbevolen wordt hierbij aan te sluiten met het verbod op geautomatiseerde besluitvorming in andere wetgeving.

Dit preadvies laat zien dat de nieuwe wetgeving voor inlichtingen- en veiligheidsdiensten aanzienlijke uitvoeringsproblemen kent en tegelijkertijd een te beperkte bescherming voor betrokken biedt bij vormen van geautomatiseerde data-analyse die een ernstige inbreuk op fundamentele rechten van betrokkenen maken. Het proces van metadata-analyse staat daarbij als voorbeeld centraal. De Commissie-Jones-Bos is verzocht de Wiv 2017 te evalueren en te rapporteren over verschillende onderwerpen die in dit artikel aan bod zijn gekomen, zoals de knelpunten in de toepassingspraktijk van de wet. De voorstellen in het preadvies dragen hopelijk bij aan het vinden van een regeling die zowel werkbaar is in de praktijk als voldoende waarborgen biedt ter bescherming van de fundamentele rechten van de betrokken personen.