*Prof. mr. dr. J.J. Oerlemans**

# Metadata-analyse in de Wiv 2017

## 282

**Metadata-analyse gaat over een vorm van data-analyse waarbij kan worden nagegaan welke telefoontoestellen met elkaar in contact zijn geweest, wanneer, en waar een communicatiemiddel zich op een bepaald moment bevond. Vanwege de ernstige privacy-inbreuk is een bepaalde vorm van metadata-analyse als een bijzondere bevoegdheid in de Wiv 2017 geregeld.**

**Deze nieuwe bijzondere bevoegdheid werkt in de praktijk niet goed en geldt niet voor andere vormen van data-analyse die een ernstige inbreuk maken op de persoonlijke levenssfeer van personen. Dit artikel analyseert deze problematiek en biedt twee oplossingsrichtingen voor een betere regeling voor metadata-analyse in de Wiv 2017.**

### 1 Inleiding

Over 'metadata-analyse' is in Nederland en in het buitenland veel maatschappelijke discussie geweest. 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).[1] 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.[2]

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.[3] 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.[4]

In de Wiv 2002 was het analysen van metadata 'lastenvrij', wat wil zeggen dat hiervoor geen bijzondere bevoegdheden met een voorafgaande toets op noodzakelijkheid, proportionaliteit en subsidiariteit was vereist.[5] In de nieuwe Wet op inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) is voor het gebruik van metadata-analyse uit 'onderzoeksopdrachtgerichte interceptie' (hierna: bulkinterceptie) als bijzondere bevoegdheid geregeld.[6]

In de praktijk blijkt nu echter dat de nieuwe bijzondere bevoegdheid tot metadata-analyse zeer beperkt wordt toegepast, namelijk slechts voor het doeleinde van 'force protection'.[7] Force protection gaat over de bescherming van militairen in missiegebieden, zoals het identificeren en lokaliseren van vijandelijke eenheden.[8] Deze beperkte toepassing is onwenselijk, omdat metadata-analyse een belangrijk instrument is ter bescherming van de nationale veiligheid. De mogelijkheid bestaat dat hierdoor personen die een bedreiging vormen voor de nationale veiligheid niet worden geïdentificeerd.

In dit artikel staat daarom de vraag centraal op welke wijze de regeling van 'metadata-analyse' kan worden verbeterd in Wiv 2017. Het gaat daarbij om een regeling die 'werkbaar' is voor de AIVD en de MIVD, maar ook voldoende waarborgen biedt ter bescherming van de fundamentele rechten van de betrokkene. De Commissie-Jones-Bos is 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 artikel aan bod komen, zoals de knelpunten in de toepassingspraktijk van de wet. Ten tijde van het verschijnen van dit artikel is het rapport van de evaluatiecommissie nog niet gepubliceerd. De voorstellen in dit artikel kunnen bijdragen aan het vinden van een regeling die zowel

---

* Jan-Jaap 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). Dit artikel is gebaseerd op het preadvies 'Geautomatiseerde data-analyse door inlichtingen- en veiligheidsdiensten' voor de staatsrechtconferentie 'Staatsrecht in de datasamenleving' van 4 december 2020.

1 Zie over het debat in Nederland ook *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 (2014)).
2 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 111. Zie voor een meer uitgebreide beschrijving ook par. 3.
3 *Kamerstukken II* 2012/13, 30977, nr. 71.
4 Zie *Kamerstukken II* 2016/17, 34588, nr. 3, p. 93.
5 Zie CTIVD-rapport nr. 38 (2014), p. 14.
6 Art. 50 lid 1 onder b jo. lid 4 Wiv 2017.
7 Zie CTIVD-rapport nr. 62 (2019) en 69 (2020) (Voortgangsrapportage II en IV Implementatie Wiv 2017).
8 Zie bijvoorbeeld CTIVD-rapport nr. 44 (2015) over MIVD-operaties op het gebied van piraterijbestrijding in de Hoorn van Afrika.

werkbaar is in de praktijk, als voldoende waarborgen biedt ter bescherming van de fundamentele rechten van de betrokken personen.

Ter beantwoording van de onderzoeksvraag wordt eerst de nieuwe regeling voor metadata-analyse en de problematiek diepgaander onderzocht. Vervolgens wordt een oplossingsrichting voorgesteld. Daarbij komen ook de nadelen van een andere regeling aan bod. Het artikel sluit af met een conclusie.

## 2 Metadata-analyse in artikel 50

Voor metadata-analyse die wordt uitgevoerd na de inzet van bulkinterceptie (artikel 48 Wiv 2017) moet een bijzondere bevoegdheid worden ingezet (artikel 50 lid 1 onder b jo. lid 4 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 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'.[9] Metadata-analyse kan dus informatie opleveren over de bekende targets en over andere, nog onbekende targets.[10] 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.

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 gebruikmaken van uitgebreide visualisatietechnieken.[11]

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.[12] Uit jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) in (o.a.) de zaken *Liberty e.a.*[13], *Brother Watch e.a.*[14](met betrekking tot bulkinterceptie) en het Hof van Justitie van de Europese Unie (HvJ EU) in de zaken *Digital Rights,*[15] *Tele2 Sverige en AB/Watson,*[16] *Privacy International,*[17] en de samengevoegde zaken van *La Quadrature du Net e.a.*[18] 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. Daar 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.[19] 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.[20]

Het onderliggende doel van bijzondere bevoegdheden is om betrokkenen te beschermen tegen het misbruik van overheidsmacht, in dit geval de AIVD en de MIVD. In de Wiv gaat het daarbij om de bescherming tegen willekeur bij inbreuken op (met name) de persoonlijke levenssfeer van personen vanwege de inzet van de bevoegdheden. Het regelen van inlichtingenmethoden in de wet maakt duidelijk wat AIVD en de MIVD precies mogen onder welke omstandigheden en voorkomt daarmee willekeur.[21] Het fungeert hier ook als toetsingsmaatstaf voor het optreden van de overheid en vormt de basis voor

9 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 111.
10 Een 'target' is een persoon of organisatie waar de AIVD of de MIVD onderzoek naar verricht.
11 CITVD-rapport nr. 38 (2014), p. 28.
12 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.
13 EHRM 1 juli 2008, nr. 58243/00, ECLI:CE:ECHR:2008:0701JUD005824300, par. 69 (*Liberty e.a./Verenigd Koninkrijk*).
14 EHRM 13 september 2018, nr. 58170/13, 62322/14, 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013, par. 356-357 (*Big Brother Watch e.a./Verenigd Koninkrijk*, sinds februari 2019 aanhangig bij de Grote Kamer).
15 HvJ EU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238, par. 27 (*Digital Rights/Ierland*).
16 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*).
17 HvJ EU 6 oktober 2020, C-623-17, ECLI:EU:C:2020:790, par. 70-73 (*Privacy International/Verenigd Koninkrijk*).
18 HvJ EU 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, par. 117 en 153 (*La Quadrature du Net e.a./Frankrijk*).
19 *BigBrother Watch e.a.*, par. 346-347 en 357.
20 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 111.
21 Zie ook *Kamerstukken II* 1997/98, 25877, nr. 3, p. 2. De regels dienen hiermee ook rechtszekerheid van betrokkenen. Zie ook A.J. Nieuwenhuis, 'Tussen geheimhouding en controle: de AIVD in de democratische rechtsstaat', *TvCR* 2016, afl. 2, p. 79-98.

controle op dit handelen van de AIVD en de MIVD.[22] Indirect kan het werk van de inlichtingen- en veiligheidsdiensten ook andere grote gevolgen hebben voor mensen, waaronder aanhouding voor een strafbaar feit. In Nederland hebben inlichtingen- en veiligheidsdiensten geen bevoegdheid personen te arresteren, maar de diensten kunnen via 'ambtsberichten' andere overheidsinstellingen informeren over mogelijke dreigingen van de nationale veiligheid. Door een ambtsbericht naar het Openbaar Ministerie kan de politie onder leiding van het OM een opsporingsonderzoek starten en eventueel tot aanhouding overgaan. Het verstrekken van ambtsberichten en de verwerking van gegevens is daarom ook gereguleerd in de Wiv 2017.

Gegevensverwerkingen zijn genormeerd door de algemene bepalingen omtrent gegevensverwerking in artikel 18-24 Wiv 2017. De verwerking vindt slechts plaats voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede uitvoering van de Wiv 2017 of de Wet veiligheidsonderzoeken. Bovendien dient de verwerking te geschieden in overeenstemming met de wet en op zorgvuldige wijze. Metadata-analyse wordt daarbij in de Wiv 2017 gezien als een vorm van geautomatiseerde data-analyse. In artikel 60 Wiv 2017 is te lezen dat geautomatiseerde data-analyse in ieder geval omvat: (a) het op geautomatiseerde wijze onderling vergelijken van gegevens, (b) het doorzoeken van gegevens aan de hand van profielen, en (c) het vergelijken van gegevens met het oog op het opsporen van bepaalde patronen. Geautomatiseerde data-analyse varieert dus van een eenvoudige (feitelijke) zoekslag, het gebruik van een applicatie om gegevens uit verschillende interne bronnen te vergelijken, tot 'profiling' op basis van gegevensbestanden en het gebruik van technieken als 'machine learning'.

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'.[23] Het ligt voor de hand dat voor verwerkingen die een grotere inmenging vormen op de rechten en vrijheden van de betrokkenen, meer waarborgen worden toegepast, ook vanwege de zorgplicht met betrekking tot gegevensverwerking (artikel 24 Wiv 2017).[24] Als waarborg kan worden gedacht aan het beperken van toegang tot bepaalde data of bepaalde functionaliteiten bij gegevensverwerkingen, het verwijderen van gegevens en het stellen van bewaartermijnen voor gegevens.

De huidige bijzondere bevoegdheid voor metadata-analyse als bijzondere bevoegdheid in artikel 50 Wiv 2017 kent mijns inziens twee problemen: (1) het is lastig uitvoerbaar en (2) de reikwijdte van de regeling is te beperkt.

### 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.[25] Bij de inzet van deze bijzondere bevoegdheid voert de Toetsingscommissie Inzet Bevoegdheden (TIB) een rechtmatigheidsoordeel uit op de verleende toestemming van de minister. 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.[26] De aanvraag moet ook voldoen aan de vereisten in de bijzondere bevoegdheid zelf. De aanvraag tot inzet van de bijzondere bevoegdheid tot metadata-analyse moet ook (a) een aanduiding bevatten van de toe te passen vorm van geautomatiseerde data-analyse en (b) een aanduiding bevatten van de gegevensbestanden die in de geautomatiseerde data-analyse worden betrokken.[27]

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.[28] 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. Eén 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

22 G.J. Veerman, *Over wetgeving. Principes, paradoxen en praktische beschouwingen*, Den Haag: Sdu Uitgevers 2012, p. 25.
23 *Kamerstukken II* 2016/17, 34588, nr. 18, p. 22.
24 In de MvT staat dat bij het gebruik van 'nieuwe technieken voor geautomatiseerde data-analyse', een dergelijke voorafgaande verkenning op de voor- en nadelen en mogelijke privacyrisico's plaatsvindt (*Kamerstukken II* 2016/17, 34588, nr. 3, p. 132).
25 Art. 50 lid 1 onder b jo. lid 4 Wiv 2017.
26 Zie art. 26 en art. 29 Wiv 2017.
27 In de MvT staat aangegeven dat in de praktijk de metadata wordt gecorreleerd met andere gegevensbestanden die de diensten ter beschikking hebben. Het is van belang deze gegevensbestanden te duiden, omdat deze van belang is om aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit te toetsen. *Kamerstukken II* 2016/17, 34588, nr. 3, p. 112.
28 *Kamerstukken II* 2017/18, 34588, nr. 70.

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.[29] Bovendien richt de toets zich klaarblijkelijk op de verwerving (de verzameling van gegevens). Het is 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 goede aanvragen te formuleren voor de inzet van de bijzondere bevoegdheid van metadata-analyse uit bulkinterceptie.[30] 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 worden betrokken. In de praktijk worden gegevens geautomatiseerd met elkaar vergeleken in verschillende databronnen (de 'naslag in geïntegreerde gegevensbronnen') en met behulp van applicaties wordt bijvoorbeeld nagegaan wie met wie bellen (een netwerkanalyse). Daarnaast geeft de memorie van toelichting aan dat tot op zekere hoogte het verplaatsingsgedrag en het surfgedrag 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 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 in de taakuitvoering (de bescherming 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. 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 onder 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.[31] 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.

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. 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) is ook vreemd. 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 de nieuwe Wiv wordt ook opgemerkt dat ook bij de verwerking van andersoortige gegevens dan telecommunicatiegegevens, zoals reisgegevens en financiële gegevens, een ernstige privacy-inbreuk kan plaatsvinden, waar voldoende waarborgen tegenover moeten staan.[32]

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.

---

29 *Kamerstukken II* 2018/19, 35242, nr. 3, p. 4-5.
30 CTIVD-rapport nr. 69 (2020) (Voortgangsrapportage IV Implementatie Wiv 2017) (augustus 2020).
31 Zie CTIVD-rapport nr. 63 (2019) over de toepassing van filters bij OOG-interceptie door de AIVD en MIVD.
32 Zie B.J. Koops e.a., 'Privacy Impact Assessment Wet op de inlichtingen-en veiligheidsdiensten 20XX', *TNO/TILT* 2016, p. 63.

## 3 Oplossingsrichting 1: combinatie met selectie van gegevens

Een oplossing voor de geschetste problematiek in paragraaf 2.1 over de lastige uitvoerbaarheid van de aanvraag 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. 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.[33]

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'.[34] Het blijkt in de praktijk lastig onderscheid te maken tussen inhoud en metadata bij internetverkeer.[35] Het is bijvoorbeeld onduidelijk of de URL naar een website als inhoud of metadata moet worden gezien.[36]

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.[37] 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. Een nieuwe regeling moet wel voldoen aan de minimale waarborgen die vanuit het EHRM en het HvJ EU worden geformuleerd bij de verzameling en verwerking van bulkgegevens. Deze jurisprudentie is nog in ontwikkeling en wordt aan het einde van de volgende paragraaf nader onderzocht.

33 Zie uitgebreid CTIVD-rapport nr. 64 (2019) over de inzet van de bijzondere bevoegdheid tot selectie door de AIVD en de MIVD.
34 *Stb.* 2017, 116. Zie ook *Kamerstukken II* 2016/17, 34588, 3, p. 111.
35 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*, Nijmegen: Wolf Legal Publishers (WLP) 2014.
36 CTIVD-rapport nr. 64 (2019), p. 13.
37 Zie J.J. Oerlemans, 'Grenzen stellen aan datahonger. De bescherming van de nationale veiligheid in een democratische rechtsstaat', inaugurele rede, Universiteit Utrecht 2020.

## 4 Oplossingsrichting 2: specifieke regels als uitwerking zorgplicht

De tweede oplossing voor de problematiek in paragraaf 2.2 over de beperkte reikwijdte is om de bijzondere bevoegdheid tot metadata-analyse in artikel 50 lid 1 onder b Wiv 2017 te schrappen en nadrukkelijk invulling te geven aan de algemene bepalingen voor gegevensverwerking als een ernstige inbreuk op het recht op privacy van personen plaatsvindt. Vanuit de zorgplicht in artikel 24 Wiv 2017 moet het hoofd van de AIVD en de MIVD technische, personele en organisatorische maatregelen treffen in verband met de verwerking van gegevens.[38] Daarbij moet op grond van artikel 24 lid 2 onder b Wiv 2017 aandacht zijn voor de gehanteerde algoritmen en modellen en kunnen op grond artikel 24 lid 2 onder c Wiv 2017 personen worden aangewezen die bij uitsluiting van anderen bevoegd zijn de gegevens te verwerken.

Met de tweede oplossing moeten de diensten in de eerste plaats zelf een regeling treffen en deze in technische systemen implementeren om een zorgvuldige gegevensverwerking te waarborgen. 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.[39] 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.[40] De diensten zouden ook per dataset kunnen bepalen voor welke taken de gegevens mogen worden verwerkt.

Het ligt daarbij voor de hand specifieke maatregelen te nemen voor gegevensverwerkingen die een ernstige inbreuk op het recht op privacy en het recht op bescherming van gegevens kunnen maken. 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.

Een voorbeeld van specifiek beleid vormt de 'Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017', die op 5 november 2020 is gepubliceerd.[41] 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. 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 tot het bewaren van de bulkdataset.[42]

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- en HvJ EU-jurisprudentie wel een belangrijke factor is om de ernst van de privacy-inmenging te meten.[43]

De toegang tot gegevens in bulkdatsets is met de regeling ingedeeld in een (a) standaard toegangsregime, (b) beperkt toegangsregime of (c) strikt beperkt toegangsregime. Onder het standaard toestemmingsregime 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 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 zich daarin een kenmerk bevindt, zoals een

38 Zie art. 24 Wiv 2017. De bepaling is opgenomen naar aanleiding van een aanbeveling uit de 'Privacy Impact Assessment Wet op de inlichtingen- en veiligheidsdiensten 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).
39 De taken van de AIVD en de MIVD worden in art. 8 en art. 10 Wiv 2017 benoemd.
40 Art. 28 Wiv 2017. De zogenoemde a- en d-taak staan in art. 8 Wiv 2017 (voor de AIVD).
41 *Stcrt.* 2020, 56482.
42 In dit artikel wordt niet ingegaan op de regeling voor de verstrekking van bulkdatasets aan een buitenlandse inlichtingen- en veiligheidsdienst.
43 EHRM 2 september 2010, nr. 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305, par. 45 (*Uzun/Germany*). 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./Frankrijk*).

telefoonnummer.[44] De periodieke beoordeling vindt plaats om de 3 jaar, 2 jaar, of 1 jaar; afhankelijk van het type bulkdataset. Dan wordt beoordeeld of de dataset moet worden verwijderd.

In de tijdelijke 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.

In de *Big Brother Watch*-zaak lijkt het EHRM wel ruimte te bieden voor een regeling zonder voorafgaande toestemming voor metadata-analyse op de onderschepte gegevens. Dan moet naar het gehele systeem worden gekeken met alle 'checks and balances' die misbruik van de bevoegdheden moeten tegengaan.[45] Als 'check and balance' verdient het overweging de CTIVD een bindend oordeel te laten geven en daarmee een interventiebevoegdheid te geven bij onrechtmatige gegevensverwerkingen.[46] 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.[47] 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.*[48] komt het Hof van Justitie tot de conclusie dat zij zich ook kan uitspreken over de verwerking van (bulk)gegevens door aanbieders van elektronische communicatiediensten ten behoeve van inlichtingen- en veiligheidsdiensten.[49] 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 Europese Unie.[50] Het HvJ EU acht 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.[51] 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 mag plaatsvinden uitsluitend op basis van gevoelige gegevens en benadrukt het verbod op geautomatiseerde besluitvorming zonder menselijke toets.[52] Afgezien van het ontbreken van een bindend element bij gegevensverwerking, lijkt de Wiv 2017 met betrekking tot het vraagstuk van metadata-analyse door de AIVD en de MIVD zelf geen aanpassing te behoeven.

## 5 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. Verder kan zich ook bij andere verwerkingen van persoonsgegevens

eveneens een ernstige inbreuk op de persoonlijke levenssfeer voordoen die specifieke waarborgen rechtvaardigt.

Het onderliggende idee is het recht op privacy beter te beschermen door een specifieke regeling te treffen voor gegevensverwerkingen die een ernstige inbreuk op de persoonlijke levenssfeer van personen maken door metadata-analyse. In dit artikel worden twee oplossingsrichtingen gepresenteerd die de huidige regeling voor metadata-analyse kunnen verbeteren, maar ook hun eigen nadelen kennen.

---

44 Zie de toelichting op de tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017.
45 *Big Brother Watch e.a.*, par. 320.
46 De CTIVD kent op dit moment alleen de mogelijkheid tot een bindend oordeel bij klachten. Zie over bindend toezicht ook art. 15 en 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./Frankrijk*, par. 139.
47 Zie in dit kader de beleidsreactie van de minister op rapport nr. 70 en nr. 71, waarbij de minister de aanbeveling bepaalde bulkdatasets te vernietigen naast zich neer heeft gelegd, vanwege de bewezen waarde van de bulkdatasets voor de taakuitvoering van de AIVD en de MIVD in het verleden.
48 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./Frankrijk*).
49 *La Quadrature du Net*, par. 99-104.
50 Art. 4 lid 2 van het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie. Zie ook Plixavra Vogiatzoglou & Jenny Bergholm, 'Privacy International & La Quadrature du Net: the latest on data retention in the name of national and public security', law.kuleuven.be 27, oktober 2020.
51 Vertaald uit de woorden 'genuine', 'present' en 'forseeable' (*La Quadrature du Net*, par. 137).
52 Zie *La Quadrature du Net*, par. 179-182.

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 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 recentelijk (november 2020) is gedaan in de 'Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017'. Als extra waarborg kan overwogen worden de CTIVD een bindend oordeel te laten 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 van de AIVD en de MIVD bij een dergelijk oordeel. Daarom kan daarbij ook worden gedacht aan een beroepsmogelijkheid van deze beslissing bij een rechterlijke instantie.

De Commissie-Jones-Bos voert een evaluatie uit op de Wiv 2017 en publiceert in 2021 haar rapport. De voorstellen in het artikel dragen hopelijk bij aan het vinden van een regeling voor metadata-analyse die zowel werkbaar is in de praktijk als voldoende waarborgen biedt ter bescherming van de fundamentele rechten van de betrokken personen.