S.J. Eskens[1]

Ongerichte interceptie, of het verwerven van bulkcommunicatie, en waarom de Grondwet en het EVRM onvoldoende tegenwicht bieden

Computerrecht 2015/85

Op basis van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (WIVD 2002) zijn de Nederlandse geheime diensten bevoegd om gegevens te verzamelen, op te slaan en te verwerken. Hieronder valt de bijzondere bevoegdheid tot ongerichte interceptie van de ether, en er komt een wetsherziening aan waarmee deze bevoegdheid wordt uitgebreid naar de kabel. De precieze uitwerking van de nieuwe wet wordt nog voorbereid, maar het kabinet benadrukt dat er acht wordt geslagen op de eisen die volgen uit onze Grondwet en het Europees Verdrag voor de rechten van de mens (EVRM). De auteur stelt dat de Grondwet en het EVRM onvoldoende tegenwicht bieden aan deze nieuwe bevoegdheid, en dat 'acht slaan op die eisen' niet volstaat.

1. Inleiding[2]

Op basis van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (WIVD 2002) zijn de Nederlandse geheime diensten bevoegd om gegevens te verzamelen, op te slaan en te verwerken. Hieronder valt de bijzondere bevoegdheid tot ongerichte interceptie van de ether, en er komt een wetsherziening aan waarmee deze bevoegdheid wordt uitgebreid naar de kabel. De precieze uitwerking van de nieuwe wet wordt nog voorbereid, maar het kabinet benadrukt dat er acht wordt geslagen op de eisen die volgen uit onze Grondwet en het Europees Verdrag voor de rechten van de mens (EVRM).[3] Daarmee is echter nog niet alles gezegd.

Deze bijdrage bevat een kritische beschouwing over de bescherming van het grondrecht op privacy door artikel 10 en 13 van de Grondwet en artikel 8 van het EVRM bij beperkingen ten behoeve van de nationale veiligheid, in het bijzonder bij ongerichte interceptie. Paragraaf 2 zet het grondrechtelijke kader uiteen en paragraaf 3 laat zien dat de WIVD 2002 en het nieuwe interceptiestelsel hieraan voldoen. Paragraaf 4 benoemt drie problemen met de waarborgen bij ongerichte interceptie zoals die volgen uit de Grondwet. Vervolgens toont paragraaf 5 dat de voorwaarden van artikel 8 van het EVRM dit niet ondervangen. De conclusie in paragraaf 6 is dat de bevoegdheid tot ongerichte interceptie inderdaad zo geregeld kan worden dat het wettelijke stelsel voldoet aan de eisen die volgen uit de Grondwet en het EVRM, maar dat die artikelen niet voldoende tegenwicht bieden aan ongerichte interceptie.

2. Het grondrecht op privacy

Ongerichte interceptie raakt met name het grondrecht op privacy en vertrouwelijke communicatie. Artikel 10, eerste lid, van de Grondwet beschermt het recht op eerbiediging van de persoonlijke levenssfeer, en staat toe dat dit recht bij of krachtens de wet beperkt wordt. Toestemming van de rechter of een minister is niet nodig. Daarnaast beschermt artikel 13, eerste lid, van de Grondwet het briefgeheim, waarbij schending slechts gerechtvaardigd is in de gevallen bij de wet bepaald, op last van de rechter. Artikel 13, tweede lid, beschermt het telefoon- en telegraafgeheim, welke geschonden kan worden in de gevallen bij de wet bepaald, door of met machtiging van een daartoe bij wet aangewezen persoon.

Sinds de opkomst van moderne communicatiemiddelen is de reikwijdte van het brief-, telefoon- en telegraafgeheim onduidelijk.[4] Uit de verscheidene plannen van de regering om álle vertrouwelijke communicatie grondwettelijke bescherming te bieden, blijkt dat email en andere digitale communicatiemedia naar de letter van de wet niet onder artikel 13 van de Grondwet vallen.[5] Toch overwoog een rechter eind jaren negentig dat het briefgeheim zich ook uitstrekt tot en met email.[6] Volgens de grondwetgever vallen verkeersgegevens niet onder artikel 13, omdat dit artikel puur de inhoud van communicatie zou beschermen.[7] Daarentegen wordt in de literatuur volgehouden dat verkeersgegevens wél onder

1 Sarah Johanna Eskens volgt de onderzoeksmaster Informatierecht aan de Universiteit van Amsterdam / Instituut voor Informatierecht (IViR).

2 Dit artikel is een vervolg op een paper dat de auteur heeft geschreven in het kader van haar master. De auteur bedankt professor Dommering en Bart van der Sloot voor hun commentaren op het paper.

3 *Kamerstukken II* 2014/15, 33820, 4, p. 6.

4 Zie hierover meer uitgebreid W.A.M. Steenbruggen, *Publieke dimensies van privé-communicatie: een onderzoek naar de verantwoordelijkheid van de overheid bij de bescherming van vertrouwelijke communicatie in het digitale tijdperk* (diss. Amsterdam UvA), Amsterdam: Otto Cramwinckel 2009, p. 249-257 en 2 p. 64-266.

5 *Kamerstukken II* 1996/97, 25443, 3 (MvT); *Kamerstukken II* 2000/01, 27460, 1; *Kamerstukken II* 2013/14, 33989, 3 (MvT).

6 Rb. Utrecht 16 september 1998, *NJK* 1998, 83.

7 *Kamerstukken II* 1996/97, 25443, 3, p. 3-4 (MvT); *Kamerstukken II* 2000/01, 27460, 1, p. 27; *Kamerstukken II* 2013/14, 33989, 3, p. 19. Zie hierover ook B.-J. Koops en J. Smits, *Verkeersgegevens en artikel 13 Grondwet, Een technische en juridische analyse van het onderscheid tussen verkeersgegevens en inhoud van communicatie*, Oisterwijk: Wolf Legal Publishers 2014, p. 75-81.

artikel 13 (zouden moeten) vallen.[8] In ieder geval genieten moderne vormen van communicatie en verkeersgegevens, voor zover dit persoonsgegevens zijn, de bescherming van het meer algemene artikel 10 van de Grondwet.

In het wetsvoorstel om de huidige geheimen te vervangen door het brief- en telecommunicatiegeheim krijgt email dezelfde bescherming als nu voor het briefgeheim geldt.[9] Verkeersgegevens komen dan onder artikel 13 van de Grondwet te vallen voor zover ze de inhoud van communicatie betreffen.[10] Daarbij moet opgemerkt worden dat een beperking op het nieuwe telecommunicatiegeheim in het belang van de nationale veiligheid, toegestaan is in de gevallen bij de wet bepaald door of met machtiging van hen die daartoe bij de wet zijn aangewezen. Wat dat betreft is aanpassing van de WIVD 2002 dus niet nodig.

Het recht op privacy in het EVRM bevat net zoals de Grondwet een beperkingsclausule, maar in tegenstelling tot de Grondwet staat het buiten twijfel dat dit recht moderne communicatiemiddelen beschermt. Onder artikel 8, eerste lid, van het EVRM heeft eenieder recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Inmenging is slechts gerechtvaardigd als deze voldoet aan drie voorwaarden, te vinden in het tweede lid: de inmenging dient een legitiem doel, bijvoorbeeld nationale veiligheid; de inmenging is noodzakelijk in een democratische samenleving in het belang van dat doel; en, de inmenging is voorzien bij wet. Het Europees Hof voor de Rechten van de Mens (het Hof) interpreteert de noties van 'correspondentie' en 'privéleven' ruim, zodat telefoongesprekken,[11] telefonieverkeersgegevens,[12] en email en internetgebruik[13] ook beschermd zijn.

3. Het huidige en nieuwe interceptiestelsel[14]

Op basis van de WIVD 2002 zijn de AIVD en de MIVD bevoegd tot *ongerichte* interceptie van niet-kabelgebonden telecommunicatie, dat is van radio- en satellietsignalen (artikel 27 lid 1 WIVD 2002), en *gerichte* interceptie van de kabel en de ether (artikel 25 lid 1 WIVD 2002). Bij ongerichte interceptie weet een inlichtingendienst niet precies wie of wat het zoekt, en onderschept het daarom alle data dat via een zeker communicatiekanaal wordt verzonden. Dit levert '*signals intelligence*' ('sigint') op. *Gerichte* interceptie ziet juist op het onderscheppen van de communicatie van een specifiek target, telefoonnummer of IP-adres, of frequentie. Hierbij maakt de wetgever onderscheid tussen 'open' en 'gesloten' communicatiemiddelen. Draadloze telecommunicatie is open, in die zin dat eenieder met de juiste apparatuur de signalen op kan vangen. Volgens de regering biedt het telefoon- en telegraafgeheim dan geen bescherming.[15]

De bevoegdheden tot gerichte en ongerichte interceptie kennen een verschillend toestemmingsmodel. Bij ongerichte interceptie van etherverkeer wordt nog geen kennis wordt genomen van de inhoud van de communicatie, waardoor er volgens de wetgever nog geen sprake is van een inbreuk op het telefoon- en telegraafgeheim, of de persoonlijke levenssfeer.[16] Daarom stelt de WIVD 2002 dat ministeriële toestemming niet vereist is.[17] Gerichte interceptie van de kabel ziet op het aftappen van besloten communicatie, en hierbij wordt wel gelijk kennisgenomen van de inhoud van de communicatie. In overeenstemming met artikel 13, tweede lid, van de Grondwet stelt de WIVD 2002 dat deze bevoegdheid slechts mag worden uitgeoefend indien de betrokken minister daarvoor toestemming heeft verleend.[18]

Met de herziening van de WIVD 2002 komt het technische onderscheid tussen kabel en ether te vervallen.[19] Het nieuwe interceptiestelsel onderscheidt drie fases. In de eerste fase zijn de AIVD en de MIVD bevoegd tot het doelgericht verwerven van bulk-communicatie. De tweede fase omvat het voorbewerken van data, en in de derde fase vindt subject gericht onderzoek plaats door middel van de verwerking van data. Per fase is opnieuw ministeriële toestemming nodig.[20] De term 'ongericht' verdwijnt uit de wet,[21] hoewel het doelgericht verwerven van bulk-communicatie naar mijn idee gewoon neer kan komen op ongerichte interceptie – tenzij het doel beperkt is tot het in bulk onderscheppen van de communicatie behorend bij een specifiek target.

De regering had er ook voor kunnen kiezen om het technische onderscheid op te heffen, en voortaan alleen gerichte vormen van interceptie en opslag toe te staan. Zo dringt de Commissie Burgerlijke vrijheden, justitie en binnenlandse zaken van het Europees Parlement er bij de regering op aan

8 J. A. Hofman, *Vertrouwelijke communicatie. Een rechts- vergelijkende studie over de geheimhouding van communicatie in grondrechtelijk perspectief naar internationaal, Nederlands en Duits recht*, Zwolle: W.E.J. Tjeenk Willink 1995; L.F. Asscher, *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving* (diss. Amsterdam UvA), Amsterdam: Otto Cramwinckel 2002; E. Dommering, 'Het derde voorstel tot een "technische neutrale" wijziging van artikel 13 Gw', *Ars Aequi* mei 2013, p. 378-285.

9 *Kamerstukken II* 2013/14, 33989, 3, p. 6 en 26 (MvT).

10 *Kamerstukken II* 2013/14, 33989, 3, p. 19 (MvT).

11 EHRM 6 september 1978, 5029/71 (*Klass e.a./Duitsland*), par. 41.

12 EHRM 2 augustus 1984, 8691/79 (*Malone/Verenigd Koninkrijk*), par. 83-84.

13 EHRM 3 april 2007, 62617/00 (*Copland/Verenigd Koninkrijk*), par. 41-42.

14 Zie voor een kritische beschouwing van de huidige WIVD 2002 ten tijde van haar totstandkoming A.H. Ekker, 'Het onderscheppen van telecommunicatie door de inlichtingen- en veiligheidsdiensten,' *Computerrecht* 2002/2, p. 77-83.

15 *Kamerstukken II* 1975/76, 13872, 3, p. 46; *Kamerstukken II* 1995/96, 24072, 14, p. 33-34. Zie hierover ook Steenbruggen 2009, p. 252.

16 *Kamerstukken II* 1997/98, 25877, 3, p. 44 (MvT). Dat er geen inbreuk is op de persoonlijke levenssfeer is overigens niet in lijn met de rechtspraak van het Hof: opslag van persoonsgegevens door de overheid is *op zichzelf* al een inmenging met het recht op privacy. Zie bijvoorbeeld EHRM 16 februari 2000, 27798/95 (*Amann/Zwitserland*), par. 69.

17 Art. 27 lid 2 WIVD 2002.

18 Art. 27 lid 2 WIVD 2002.

19 *Kamerstukken II* 2014/15, 33820, 4, p. 4-5.

20 *Kamerstukken II* 2014/15, 33820, 4, bijlage.

21 *Kamerstukken II* 2014/15, 29924, 121, p. 23.

af te zien van de geplande uitbreiding van bevoegdheden.[22] En Jacobs bepleit bijvoorbeeld een model waarbij reeds op het moment van ongerichte interceptie vluchtig de relevantie van het materiaal wordt beoordeeld, en onnodige informatie direct wordt weggegooid.[23]

4. Drie problemen met de waarborgen van de Grondwet

De volgende paragrafen benoemen drie problemen met betrekking tot de waarborgen die de Grondwet tegenover ongerichte interceptie, of het verwerven van bulk-communicatie, stelt.

4.1 *Ministeriële toestemming*

Zoals hierboven vermeld vindt ongerichte interceptie van de ether plaats zonder ministeriële toestemming, omdat de wetgever artikel 10 en 13 van de Grondwet daarop niet van toepassing acht. Het nieuwe interceptiestelsel eist wel toestemming van de minister ten aanzien van het verwerven van bulk-communicatie, en in zoverre zal de nieuwe wet dus een extra waarborg bevatten.

Het probleem is dat voorafgaande ministeriële toestemming ten aanzien van ongerichte interceptie, of ten aanzien van het verwerven van bulk-communicatie, weinig betekenis heeft. Het kabinet stelt wel dat de last van de minister een 'zo nauwkeurig mogelijk omschreven onderzoeksopdracht' bevat, maar dit kan nog steeds betekenen dat de minister bijvoorbeeld goedkeuring geeft om voor een jaar een telefoon- of internetkabel af te tappen die door vele mensen wordt gebruikt.[24] Zulke algemene toestemming is geen waardevolle waarborg voor de individuele rechtsbescherming. Dit merkte de wetgever ook op toen de WIVD 2002 werd ingediend:

> "Overigens zou het stellen van het toestemmingsvereiste ten aanzien van de uitoefening van [ongerichte interceptie van etherverkeer] geen grote inhoudelijke betekenis hebben; een dergelijke toestemming zou dan betrekking hebben op de frequentie of het satellietkanaal ten aanzien waarvan de ongerichte interceptie plaatsvindt."[25]

Dat geldt natuurlijk ook voor de kabel; ministeriële toestemming is van weinig betekenis als deze betrekking zou hebben op de kabel ten aanzien waarvan de bulk interceptie plaatsvindt.

4.2 *Selectie van sigint*

De AIVD en de MIVD zijn op basis van artikel 27, derde lid, van de WIVD 2002 bevoegd om ongericht ontvangen niet-kabelgebonden telecommunicatie te selecteren ('selectie van sigint'), zodat er kennisgenomen kan worden van de inhoud. De wetgever ziet de uitoefening van de selectiebevoegdheid als een inbreuk op het brief- en telegraafgeheim,[26] en zodoende eist de wet voorafgaand toestemming van de minister.[27] Het nieuwe interceptiestelsel bevat dezelfde waarborg.[28]

Selectie van sigint vindt plaats aan de hand van identiteitsgegevens, telefoonnummers of andere technische kenmerken (met name IP-adressen), of aan een nader omschreven onderwerp gerelateerde trefwoorden, bijvoorbeeld de ingrediënten van een bom, in diverse talen.[29] Het verzoek tot toestemming voor de selectie moet aangeven met behulp van welke gegevens selectie zal plaatsvinden, of in het geval van de trefwoorden aan de hand van welk onderwerp, en in ieder geval de reden waarom de selectie zal worden toegepast.[30]

Het punt is dat de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) heeft meermalen geoordeeld dat de AIVD en de MIVD niet zorgvuldig omgingen met de selectie van sigint. In de periode van april 2006 tot juni 2008 bestudeerde de toezichthouder per drie maanden de verzoeken van de AIVD tot toestemming voor selectie van sigint. Ze constateerde het volgende:

> "De verzoeken (...) bevatten veel nummers en technische kenmerken zonder dat wordt toegelicht op wie of waarop deze betrekking hebben. Indien wel wordt toegelicht op wie de nummers en technische kenmerken betrekking hebben, ontbreekt veelal de toelichting waarom de persoon of organisatie in de gaten dient te worden gehouden in het kader van het onderzoek (doel) en een afweging omtrent de noodzakelijkheid, proportionaliteit en subsidiariteit."[31]

Na dit rapport is de CTIVD de uitoefening van de selectiebevoegdheid door de AIVD per kwartaal in de gaten blijven houden en heeft ze dit op een gegeven moment omgezet in een jaarlijks terugkerend diepteonderzoek. Hiervoor nam zij kennis van alle toestemmingsverzoeken, en keek ze in het bijzonder naar de zaken die gelet op het specifieke karakter van de inbreuk nader onderzoek nodig hadden. In de hier op volgende rapporten kwam ze tot dezelfde constate-

22 Resolutie van het Europees Parlement van 12 maart 2014 over het surveillanceprogramma van de NSA in de VS, toezichthoudende instanties in verschillende lidstaten en gevolgen voor de grondrechten van EU-burgers en voor de trans-Atlantische samenwerking op het gebied van justitie en binnenlandse zaken, P7_TA-PROV(2014)0230, par. 24.

23 B. Jacobs, 'Vluchtig en stelselmatig, een bespreking van interceptie door inlichtingen- en veiligheidsdiensten', 5 februari 2014, njb.nl/blog/vluchtig-en-stelselmatig-een-bespreking-van.13474.lynkx (laatst geraadpleegd op 7 mei 2015)

24 *Kamerstukken II* 2014/15, 33820, 4, p. 4.

25 *Kamerstukken II* 1997/98, 25877, 3, p. 44 (MvT).

26 *Kamerstukken II* 1997/98, 25877, 3, p. 44-45 (MvT).

27 Art. 27 lid 4 en 5 WIVD 2002.

28 *Kamerstukken II* 2014/15, 33820, 4, bijlage: Diagram hoofdlijnen nieuw interceptiestelsel.

29 Art. 27 lid 3 sub a-c WIVD 2002.

30 Art. 27 lid 4 en 5 WIVD 2002.

31 CTIVD, *Toezichtsrapport inzake de toepassing door de AIVD van artikel 25 WIV 2002 (aftappen) en artikel 27 WIV 2002 (selectie van ongericht ontvangen niet-kabelgebonden telecommunicatie)*, februari 2009 (nr. 19), p. 31. Alle rapporten zijn verkrijgbaar via www.ctivd.nl.

ringen.[32] Ook met betrekking tot de MIVD concludeerde de toezichthouder in een rapport uit 2011 dat de motivering van de verzoeken om toestemming voor selectie van sigint 'in veel gevallen onvoldoende' was.[33] Vorig jaar vroeg de toezichthouder opnieuw tweemaal nadrukkelijk aandacht voor deze problematiek bij de diensten.[34]

Wanneer de AIVD en de MIVD het gebruik van selectiecriteria niet goed motiveren, nemen ze in die gevallen in feite op willekeurige basis kennis van de inhoud van communicaties. De CTIVD, noch de interne juridische afdeling kan dan controleren of de selectie gerechtvaardigd is. Desondanks gaf de minister gewoon toestemming om te selecteren op basis van de in verzoeken opgenomen criteria.[35] In reactie op deze toezichtsrapporten gaf de betrokken minister meermalen aan dat de praktische uitvoerbaarheid van de motiveringsplicht in het oog dient te worden gehouden.[36] Hoewel het in al deze rapporten uitsluitend ging om de selectie van ongericht ontvangen etherverkeer, is het de vraag in hoeverre het wel praktisch uitvoerbaar is om de selectie van ongericht ontvangen kabelverkeer goed te motiveren. Het lijkt erop dat enige willekeur inherent is aan selectie van bulk interceptie en dat ministeriële toestemming niet waarborgt dat selectie zorgvuldig gebeurt.

4.3 *Metadata-analyse*

Na interceptie vindt met behulp van applicaties zogeheten 'metadata-analyse' plaats. Dit omvat het zoeken naar relevante verbanden en data in een verzameling verkeersgegevens, en het combineren van reeds beschikbare informatie.[37] De inzet van metadata-analyse wordt gebaseerd op de algemene wettelijke bevoegdheid tot gegevensverwerking in artikel 12, eerste lid, van de WIVD 2002, en hiervoor is geen aanvullende toestemming vereist. In het nieuwe interceptiestelsel kan metadata-analyse plaatsvinden in zowel de tweede (voorbewerken) als de derde fase (verwerken).

In een toelichting op het nieuwe interceptiestelsel gaf Plasterk het volgende voorbeeld van metadata-analyse. In de eerste fase van interceptie worden telefonieverkeersgegevens in bulk verzameld. Dan wordt deze dataset in de tweede fase vergeleken met een lijst telefoonnummers van mensen van wie bekend is dat ze 'kwade bedoelingen' hebben. Dit is een vorm van metadata-analyse. Het resultaat toont dan meestal dat de reeds bekende nummers inderdaad met elkaar in contact staan, maar het is met name de bedoeling om nieuwe mogelijk interessante telefoonnummers in een netwerk te ontdekken. In de derde fase plaatst de dienst dan bijvoorbeeld een tap op zo'n nieuw nummer.[38]

Maar, metadata-analyse kent veel meer toepassingen dan het voorbeeld van de minister. De AIVD en de MIVD zijn namelijk ook bevoegd om bij telecomproviders verkeersgegevens, inclusief locatiegegevens, en gebruikers- of abonneegegevens op te vragen, zonder toestemming van de minister.[39] Verder kunnen de diensten data opvragen bij andere instanties,[40] en uit open bronnen halen. Dit betekent dat de diensten ongericht geïntercepteerde metadata kunnen verrijken met vele soorten gegevens. Zo kan metadata-analyse gebruikt worden om gerichte observaties te genereren: hoe laat arriveert iemand op een bepaalde locatie, met wie had hij of zij van tevoren contact, en – als bulk interceptie van internetverkeer straks ook mogelijk is – naar welke Wikipedia pagina's en online winkels surfte hij of zij die avond?[41] Gerichte observatie en van natuurlijke personen en in het kader daarvan vastleggen van gegevens betreffende gedragingen is apart in de wet geregeld, en vereist toestemming van de minister.[42] Verder blijkt uit de wetgeschiedenis van de WIVD 2002 dat de diensten verzamelde data ook doorzoeken op profielen.[43] Dit betekent dat metadata-analyse veel meer informatie op kan leveren, dan in het voorbeeld van de minister, en op dit moment van weinig waarborgen is voorzien.

Het is een kleine vooruitgang dat in het nieuwe interceptiestelsel metadata-analyse waarbij wordt beoogd subjecten te identificeren wordt onderworpen aan ministeriële toestemming,[44] maar dit is geen afdoende waarborg. Al een paar jaar na de invoering van de WIVD 2002 kwam het kabinet met een voorstel de wet te wijzigen. Een van de redenen was dat de wet onvoldoende expliciet was over sommige vormen van gegevensverwerking, zoals data-analyse, waaronder het doorzoeken aan de hand van profielen.[45] Dat betekende niet dat de AIVD en de MIVD tot dan toe niet aan data-analyse deden. 'De diensten hebben al geruime tijd ervaring met data-analyses op grote hoeveelheden gegevens, (...), maar de regering [heeft] ervoor gekozen deze mogelijkheid thans ook expliciet in de wet op te nemen teneinde zodoende de kenbaarheid te vergroten en de toepassing ervan op onderdelen met extra waarborgen te omgeven."[46] Uiteindelijk werd het voorstel ingetrokken. Dit roept de vraag op of metadata-analyse en het doorzoeken op profielen, met het oog op huidige en toekomstige toepassingen, in een

32 Zie de toezichtsrapporten nr. 26, 31, 35 en 40. Op dit moment loopt het vierde jaarlijkse diepteonderzoek, over de periode maart 2014 t/m februari 2015.
33 CTIVD, *Toezichtsrapport inzake de inzet van sigint door de MIVD, 23 augustus 2011* (nr. 28), p. 54.
34 CTIVD, *Toezichtsrapport inzake de gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD*, 5 februari 2014 (nr. 38), p. 17; CTIVD, *Reactie CTIVD op het rapport commissie-Dessens*, 11 maart 2014, verkrijgbaar op www.ctivd.nl.
35 CTIVD, Toezichtsrapport nr. 19, p. 31.
36 *Kamerstukken II* 2008/09, 29924, 29, p. 6; *Kamerstukken II* 2011/12, 29924, 74, p. 2; *Kamerstukken II* 2013/14, 29924, 101, p. 3.
37 CTIVD Toezichtsrapport nr. 38, p. 14 en 19.
38 *Kamerstukken II* 2014/15, 29924, 121, p. 18-19 (Verslag Algemeen Overleg van 10 februari 2015). Zie ook *Kamerstukken II* 2012/13, 30977, 71, p. 25-26, waar Minister Plasterk 'metadatamining' uitlegt, d.w.z. metadata-analyse.
39 Art. 28 en 29 WIVD 2002 jo Besluit ex artikel 28 WIVD 2002, *Stb.* 2005, 289.
40 Art. 17 WIVD 2002.
41 Zie hierover ook de notitie 'Cyberintelligence en publiek belang', voorbereid door het Rathenau Instituut voor een expertmeeting in de Eerste Kamer, mei 2014, verkrijgbaar via *www.eerstekamer.nl/nieuws/20140507/deskundigenbijeenkomst* (laatst geraadpleegd op 7 mei 2015).
42 Art. 20 lid 1 en 3 WIVD 2002.
43 *Kamerstukken II* 2005/06, 30533, 3, p. 24-27 (MvT).
44 *Kamerstukken II* 2014/15, 33820, 4, p. 5.
45 *Kamerstukken II* 2005/06, 30553, 3, p. 13 (MvT).
46 *Kamerstukken I* 2005/06, 30553, C, p. 12.

nieuwe Wiv niet alsnog nader geregeld zou moeten worden, teneinde de kenbaarheid te vergroten en met extra waarborgen te omgeven.

6. Drie problemen met de voorwaarden van het EVRM

Het Europees Hof voor de Rechten van de Mens heeft zich pas twee keer uitgesproken over ongerichte interceptie ('*strategic monitoring*'), namelijk in de ontvankelijkheidsbeslissing van *Weber en Saravia/Duitsland* en in de zaak *Liberty e.a./Verenigd Koninkrijk*.[47] In de volgende paragrafen wordt per element van artikel 8, tweede lid, van het EVRM (zie paragraaf 2), aangetoond dat de eisen die daaruit voortvloeien geen voldoende waarborgen bieden tegen ongerichte interceptie. Hierbij wordt verwezen naar *Weber en Saravia* en andere klassieke zaken van het Hof over '*secret surveillance*.'

6.1 *Legitiem doel*

Sowieso betwijfelt het Hof nooit dat een staat met ongerichte interceptie of een andere vorm van heimelijke surveillance het legitieme doel nastreeft de nationale veiligheid te beschermen en/of misdaad te voorkomen.[48] Brems merkt in een annotatie bij een andere surveillance-zaak op dat deze voorwaarde een louter formalistische kwestie is geworden.[49] Dit betekent dat er geen directe aanleiding is om te verwachten dat het Hof ooit zal oordelen dat de bevoegdheid tot ongerichte interceptie, of het verwerven van bulk-communicatie, *niet* de nationale veiligheid dient. Er kan dus gemakkelijk geclaimd worden dat aan deze eis van het EVRM is voldaan.

6.2 *Voorzien bij wet*

Volgens het Hof vereist de voorwaarde 'voorzien bij wet' dat de inmenging een grondslag heeft in het nationale recht, dat de wetgeving toegankelijk is en dat de gevolgen ervan te voorzien zijn.[50] Het Hof erkent dat het voorzienbaarheidsvereiste in de context van geheime surveillance niet zo uitgelegd kan worden dat iemand precies moet kunnen voorspellen wanneer hij onderwerp van onderzoek zal zijn, want dan zou de bevoegdheid niet meer in het geheim kunnen worden uitgeoefend. In de plaats daarvan stelt het rechtscollege dat de wet voldoende precies moet aangeven in welke omstandigheden en onder welke voorwaarden de overheid heimelijk kan surveilleren.[51] Uit de *rule of law* volgt volgens het Hof dat de wet zodanig precies moet zijn, dat de individu afdoende beschermd is tegen arbitraire machtsuitoefening.[52] Ze heeft deze uitgangspunten vertaald naar een aantal procedurele waarborgen ('*minimum safeguards*'): de wet moet (1) de misdrijven aangeven die aanleiding kunnen vormen tot inzet van de bevoegdheid; (2) een definitie geven van de categorieën personen die onderwerp kunnen zijn surveillance; (3) een beperking stellen aan de tijdsduur; (4) een procedure aangeven voor inzage, verwerking en opslag van de verzamelde gegevens; (5) voorschriften voorschrijven met betrekking tot het doorgeven van gegevens aan andere instanties; en (6) aangeven wanneer de verzamelde gegevens vernietigd mogen of moeten worden.[53]

Deze zes minimum waarborgen zijn ontwikkeld in de context van gerichte surveillance ('*individual monitoring*').[54] In *Weber en Saravia* achtte het Hof deze waarborgen impliciet ook van toepassing op ongerichte interceptie en in *Liberty* volgde het Hof deze benadering uitdrukkelijk.[55]

Het voorzienbaarheidsvereiste dat sinds *Weber en Saravia* en *Liberty* voor ongerichte interceptie geldt, is relatief laag.[56] Van de zes waarborgen zijn met name de eerste en tweede waarborg (een beschrijving van respectievelijk de misdrijven en categorieën personen) relevant om de individu te beschermen tegen willekeurige machtsuitoefening. Het Hof accepteerde echter een ruime beschrijving van de misdrijven en de categorieën personen. In *Weber en Saravia* merkte het Hof op dat de Duitse wet precies aangaf in het geval van welke misdrijven een bevel tot ongerichte interceptie kon worden afgegeven, namelijk: een gewapende aanval op Duitsland; een internationale terroristische aanslag in het land; internationale wapenhandel, of handel in verboden goederen, computer programma's en technologieën; illegale drugsimport; valsemunterij; of het witwassen van geld.[57] Verder observeerde het Hof met goedkeuring dat de wet ook aangaf welke categorieën personen afgeluisterd kunnen worden, namelijk elke Duitser die een internationaal telefoontje pleegt en in het gesprek een woord gebruikt dat te maken heeft met de misdrijven uit sectie 3(1).[58] Er zijn heel wat woorden te bedenken die daarvoor in aanmerking komen en die dus aanleiding kunnen geven tot surveillance. Toch oordeelde het Hof dat deze beschrijving nauwkeurig genoeg was om te voldoen aan het voorzienbaarheidsvereiste, om zodoende te beschermen tegen willekeurige uitoefening van de bevoegdheid tot *strategic monitoring*.[59]

In de WIVD 2002 wordt op verschillende plekken gehoor gegeven aan het voorzienbaarheidsvereiste, maar dit laat juist zien dat dit vereiste met betrekking tot ongerichte intercep-

47 EHRM 29 juni 2006, 54934/00 (*Weber en Saravia/Duitsland*), par. 78-79; EHRM 1 juli 2008, 58243/00 (*Liberty e.a./Verenigd Koninkrijk*), par. 56-57.
48 *Weber en Saravia*, par. 104; *Liberty*, par. 58. Zie voor eenzelfde oordeel met betrekking tot andere vormen van surveillance bijvoorbeeld: *Klass*, par. 46; EHRM 18 mei 2010, 26839/05 (*Kennedy/Verenigd Koninkrijk*), par. 155; EHRM 2 september 2010, 35623/05 (*Uzun/Duitsland*), par. 77; EHRM 18 april 2013, 19522/09 (*M.K./Frankrijk*), par. 29.
49 EHRM 4 mei 2002, 28341/95, *EHRC* 2000/53, m.nt. E. Brems (*Rotaru/Roemenië*).
50 *Weber en Saravia*, par. 84; *Liberty*, par. 59. Zie ook *Malone*, par. 66 en EHRM 26 maart 1987, 9248/81 (*Leander/Zweden*), par. 50.
51 *Weber en Saravia*, par. 93; *Liberty*, par. 62. Zie ook *Malone*, par. 67 en *Leander*, par. 51.
52 *Weber en Saravia*, par. 94; *Liberty*, par. 62. Zie ook *Malone*, par. 68 en *Leander*, par. 51.
53 *Weber en Saravia*, par. 95; *Liberty*, par. 62.
54 Zoals bijvoorbeeld EHRM 24 april 1990, 11105/84 (*Huvig/Frankrijk*), par. 34; EHRM 24 april 1990, 11801/85 (*Kruslin/Frankrijk*), par. 35; EHRM 30 juli 1998, 58/1997/842/1048 (*Valenzuela Contreras/Spanje*), par. 46.
55 *Weber en Saravia*, par.95-100; *Liberty*, par. 63.
56 Zie in deze zin ook B. Goold, 'Liberty and others v The United Kingdom: a new chance for another missed opportunity', *Public Law* jan. 2009, p. 5-14.
57 *Weber en Saravia*, par. 27 en 96.
58 *Weber en Saravia*, par. 97.
59 *Weber en Saravia*, par. 101.

tie geen bescherming biedt tegen willekeurige machtsuitoefening. Zo heeft de wetgever de middelen die de AIVD en de MIVD kunnen inzetten 'nader omschreven,'[60] in die zin dat deze in globale termen in de wet zijn opgenomen.[61] Daarnaast geven de taakomschrijvingen van de diensten aan in welke omstandigheden de geheime maatregelen getroffen mogen worden, wat erop neerkomt dat verschillende taken uitgeoefend kunnen worden voor het overkoepelende belang van de nationale veiligheid.[62] In aanvulling hierop moeten de betrokken Ministers jaarlijks openbaar verslag uitbrengen van de wijze waarop de diensten hun taken in het afgelopen jaar hebben verricht en daarbij de aandachtsgebieden benoemen voor het lopende jaar.[63] In het geval van ongerichte interceptie betekent dat dus dat eenieder (categorie personen, zie hierboven) kan verwachten dat surveillance hem of haar zal betreffen zodra de staat ergens een gevaar voor de nationale veiligheid signaleert (categorie misdrijven, zie hierboven). Zo wordt geen recht gedaan aan het voorzienbaarheidsvereiste.

Er bestaat dus een onoplosbare spanning tussen ongerichte interceptie en het criterium 'voorzien bij wet,' met als gevolg dat de wetgever wederom gemakkelijk kan stellen dat aan dit vereiste van het EVRM is voldaan. Het Hof heeft het voorzienbaarheidsvereiste ingevuld met procedurele waarborgen, die ongerichte interceptie niet daadwerkelijk 'te voorzien maken.' Zo overwoog de rechtbank in *Burgers t. Plasterk* ook dat 'de ongerichte interceptie van kabelgebonden telecommunicatie, mits met voldoende waarborgen omkleed, aan de voorzienbaarheidstoets van artikel 8, tweede lid, van het EVRM kan voldoen.'[64] Door te focussen op waarborgen in plaats van op proportionaliteit, biedt artikel 8 van het EVRM uiteindelijk geen echte, fundamentele bescherming tegen omvangrijke machtsuitoefening door de overheid.[65]

6.3 *Noodzakelijk in een democratische samenleving*

Het Hof geeft de staat in het algemeen een redelijk ruime beoordelingsvrijheid met betrekking tot het noodzakelijkheidsvereiste.[66] Uiteraard houdt het Hof wel toezicht, en in dat opzicht verlangt ze dat er in de nationale rechtsorde adequate en effectieve garanties tegens machtsmisbruik bestaan.[67] Deze beoordeling hangt af van de omstandigheden van het geval, zoals: i) de soort surveillance; ii) de omvang van de bevoegdheid en de duur waarvoor deze kan worden ingezet; iii) de reden waarvoor surveillance bevolen kan worden; iv) de verschillende autoriteiten die goedkeuring moeten geven, de orders uit moeten voeren, en toezicht moeten houden en; v) de rechtsmiddelen die de burger ter beschikking staan.[68]

Van de twee zaken over ongerichte interceptie, kwam het Hof alleen in *Weber en Saravia* toe aan de noodzakelijkheidstoets, en die zaak laat zien dat bovengenoemde omstandigheden afleiden van waar het bij deze voorwaarde om zou moeten gaan: de proportionaliteitsvraag. In de betreffende zaak merkte het Hof op dat *strategic monitoring* een brede bevoegdheid is, maar volgens het Hof werd hier aan tegemoetgekomen doordat de Duitse wet een aantal voorwaarden stelde aan de inzet van de bevoegdheid, zoals het vermoeden van een ernstig misdrijf.[69] Dat lijkt mij meer een vraag van voorzienbaarheid. Daarnaast keek het Hof met name naar de procedurele inbedding, namelijk de manier waarop een bevel tot surveillance wordt afgegeven, controle op de uitvoer van zo'n bevel, en de aanwezigheid van onafhankelijke toezicht.[70] Van der Sloot schreef dat de proportionaliteitstoets naar de achtergrond is verdwenen,[71] en *Weber en Saravia* is daar een voorbeeld van.

Overigens moet hierbij worden aangetekend dat het EVRM een '*living instrument*' is,[72] zodat het niet onvoorstelbaar is dat het Hof in nieuwe zaken anders naar *strategic monitoring* zal kijken. Het Hof van Justitie van de Europese Unie oordeelde recent bijvoorbeeld dat ruime bevoegdheden tot gegevensbewaring en de toegang daartoe door de overheid, niet proportioneel was ten opzichte van het recht op privacy zoals beschermd door het Handvest van de Europese Unie.[73] Als het Europees Hof voor de Rechten van de Mens hierbij aansluiting zoekt, kan dat betekenen dat de proportionaliteitseis van artikel 8 EVRM weer naar voren treedt.

7. Conclusie

Uit de voorgaande bespreking komt het volgende naar voren. Op basis van de WIVD 2002 zijn de AIVD en de MIVD bevoegd om niet-kabelgebonden telecommunicatie ongericht te intercepteren. Deze bevoegdheid wordt binnenkort vervangen door de algemene bevoegdheid tot het verwerven van bulk-communicatie, waarmee de bevoegdheid tot ongerichte interceptie feitelijk van de ether naar de kabel wordt uitgebreid.

Artikel 10 en 13 van de Grondwet en artikel 8 van het EVRM stellen een aantal waarborgen tegenover ongerichte interceptie, in de rechtspraak van het Hof aangeduid met '*strategic monitoring*,' maar deze voorwaarden bieden onvoldoende tegenwicht aan deze bevoegdheid. Zo heeft voor-

60 *Kamerstukken II* 1997/1998, 25877, 3, p. 2-3.
61 Zie bijvoorbeeld artikel 27 WIVD 2002 voor ongerichte interceptie.
62 Art. 6 en 7 WIVD 2002 en *Kamerstukken II* 1997/1998, 25877, 14, p. 5-6.
63 Art. 8 WIVD 2002 en *Kamerstukken II* 1997/1998, 25877, 14, p. 5-6.
64 Rb. Den Haag 23 juli 2014, ECLI:NL:RBDHA:2014:8966, *Computerrecht* 2014/186, m.nt. R. van den Hoven van Genderen ('*Burgers/Plasterk*'), r.o. 5.30.
65 Zie in deze zin ook P. De Hert, 'Balancing security and liberty within the European human rights framework: A critical reading of the Court's case law in the light of surveillance and criminal law enforcement after 9/11', *Utrecht Law Review* (1) 2005, 1, p. 68–96.
66 Zie bijvoorbeeld *Klass*, par. 49; *Leander*, par. 59; *Malone*, par. 81; EHRM 6 juni 2006, 62332/00 (*Segerstedt-Wiberg/Zweden*), par. 104.
67 *Klass*, par. 50; *Weber en Saravia*, par. 106.
68 *Klass*, par. 50; *Weber en Saravia*, par. 106.
69 *Weber en Saravia*, par. 115.
70 *Weber en Saravia*, respectievelijk par. 115-117.
71 Zie hierover ook B. van der Sloot, 'Privacy in het post NSA-tijdperk', *NJB* 2014/866, afl. 17, p. 1171-1179.
72 EHRM 25 april 1978, 5856/72 (*Tyrer/Verenigd Koninkrijk*), par. 31.
73 HvJ EU 8 april 2014, in de gevoegde zaken C-293/12 en C-594/12 (*Digital Rights Ireland*).

afgaande toestemming van de minister geen grote inhoudelijke betekenis wat betreft het ongericht ontvangen van telefonie- of internetverkeer dat wordt verzonden via een zekere frequentie, of kabel. Daarnaast blijkt dat de selectie van ongericht ontvangen gegevens in de praktijk lastig te motiveren valt, terwijl de minister wel toestemming geeft om deze bevoegdheid in te zetten. Verder wordt metadata-analyse door minister Plasterk omschreven als een redelijk onschuldige praktijk, terwijl deze manier van gegevensverwerking zeer precieze informatie op kan leveren en ook *profiling* omvat. Zulke data-analyse kan reeds gebaseerd worden op de algemene bevoegdheid tot het verwerken van gegevens, maar het verschil tussen Plasterks voorbeeld en andere mogelijke toepassingen, levert een argument op om metadata-analyse nader bij wet te regelen.

Wat betreft de waarborgen van het EVRM valt op dat het voorzienbaarheidsvereiste een lage drempel opwerpt en dat het proportionaliteitvereiste geen gewicht in de schaal legt. Het is inderdaad voor iedereen te voorzien dat ongerichte interceptie theoretisch jegens hem of haar ingezet kan worden, maar in deze uitleg biedt het voorzienbaarheidsvereiste geen bescherming tegen willekeurige machtsuitoefening. Ten slotte heeft het Hof slechts in één zaak beoordeeld of ongerichte interceptie noodzakelijk was in een democratische samenleving, en daaruit lijkt te volgen dat noodzakelijkheid vooral ziet op procedurele waarborgen, en niet op proportionaliteit. In dit opzicht is het wel hoopvol dat het EVRM dynamisch is.

Desalniettemin, als de Nederlandse wetgever het nieuwe interceptiestelsel aanbiedt met de mededeling dat acht wordt geslagen op de eisen die voortvloeien uit onze Grondwet en de jurisprudentie van het EHRM, dan nóg is een nauwkeurige analyse en debat vereist over de juiste waarborgen bij deze bevoegdheid en de proportionaliteit van de inmenging met het recht op privacy.