bureau Brandeis

DAGVAARDING

Heden, de _____ op verzoek van:

1. De heer **Bart Theophilus Nooitgedagt**, woonachtig te Amsterdam;
2. De heer **Brenno Johan Simon Aymard August Frans de Winter**, woonachtig te Ede;
3. De heer **Johannes Cornelis van Beek**, woonachtig te Amsterdam;
4. De heer **Robbert Valentijn Gonggrijp**, woonachtig te Amsterdam,
5. De heer **Mathieu Hendrik Paapst**, woonachtig te Siddeburen;
6. De **Nederlandse Vereniging voor Strafrecht Advocaten**, gevestigd te (5051 RB) Goirle, aan de Kloosterstraat 17-19, hierna ook te noemen "de NVSA";
7. De **Nederlandse Vereniging voor Journalisten**, gevestigd te (1071 DR) Amsterdam, aan de Johannes Vermeerstraat 22, hierna ook te noemen "de NVJ";
8. De **Internet Society Nederland**, gevestigd te (2595 BE) Den Haag, aan het Prins Willem-Alexanderhof 5, hierna ook te noemen "de Internet Society Nederland";
9. **Stichting Privacy First**, gevestigd te (1091 GR) Amsterdam aan de Wibautstraat 150, hierna ook te noemen "Privacy First";

voor deze zaak woonplaats kiezende te (1016 DS) Amsterdam aan de Keizersgracht 203, ten kantore van bureau Brandeis, waarvan Mr Chr.A. Alberdingk Thijm en Mr C.F.M. de Vries in deze zaak als behandelend advocaten optreden en als zodanig worden gesteld en van wie Mr Chr.A. Alberdingk Thijm te dezer zake tot procesadvocaat wordt gesteld en als zodanig zal optreden;

Heb ik,

GEDAGVAARD:

1. De **Staat der Nederlanden (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)**, zetelende te (2511 DC) Den Haag, aan de Turfmarkt 147, aldaar aan het parket van de procureur-generaal bij de Hoge Raad der Nederlanden, (2514 CV) aan de Kazernestraat 52 (verder ook te noemen: de "Staat") dit exploot gedaan en afschrift van dit

exploot:

- ❑ gelaten aan:

- ❑ achtergelaten in een gesloten envelop waarop de door de wet voorgeschreven gegevens zijn vermeld, omdat ik daar niemand aantrof aan wie ik rechtsgeldig een afschrift kon laten,

OM:

op **woensdag 27 november (de "roldatum"), des voormiddags te tien uur (10.00 uur)**, niet in persoon, maar vertegenwoordigd door een advocaat, te verschijnen in het geding ten overstaan van de rechtbank Den Haag, te houden in het gerechtsgebouw aan de Prins Clauslaan 60 (2595 AJ) Den Haag.

MET AANZEGGING DAT:

- ✓ indien gedaagde niet uiterlijk op de eerste of op een door de rechter nader bepaalde roldatum een advocaat stelt of het hierna te noemen griffierecht niet tijdig betaalt, en de voorgeschreven termijnen en formaliteiten in acht zijn genomen, de rechtbank verstek zal verlenen en de vorderingen zal toewijzen, tenzij deze haar onrechtmatig of ongegrond voorkomen;
- ✓ bij verschijning in het geding van de gedaagde een griffierecht zal worden geheven, te voldoen binnen vier weken te rekenen vanaf het tijdstip van verschijning. De hoogte van de griffierechten is vermeld in de meest recente bijlage behorend bij de Wet griffierechten burgerlijke zaken, die onder meer is te vinden op de website www.kbvg.nl/griffierechtentabel;
- ✓ van een persoon die onvermogend is, een bij of krachtens de wet vastgesteld griffierecht voor onvermogenden wordt geheven, indien hij op het tijdstip waarop het griffierecht wordt geheven heeft overgelegd:
  - een afschrift van het besluit tot toevoeging, bedoeld in artikel 29 van de Wet op de rechtsbijstand, of indien dit niet mogelijk is ten gevolge van omstandigheden die redelijkerwijs niet aan hem zijn toe te rekenen, een afschrift van de aanvraag, bedoeld in artikel 24, tweede lid, van de Wet op de rechtsbijstand, dan wel
  - een verklaring van de raad als bedoeld in artikel 1, onder b, van die wet, waaruit blijkt dat zijn inkomen niet meer bedraagt dan de bedragen, bedoeld in artikel 35, derde en vierde lid, telkens onderdelen a tot en met d dan wel in die artikelleden, telkens onderdeel e, van die wet, met dien verstande dat als gevolg van een inmiddels van kracht geworden wijziging van de Wet op de rechtsbijstand nu geldt dat de verklaring wordt verstrekt door het bestuur van de raad voor rechtsbijstand, bedoeld in artikel 2 van die wet, terwijl de bedragen waaraan het

inkomen wordt getoetst zijn vermeld in artikel 2, eerste en tweede lid, van het Besluit eigen bijdrage rechtsbijstand;

- ✓ dat eisers, gelet op het spoedeisende karakter van de zaak, niet zullen meewerken aan een verzoek om uitstel voor het indienen van de conclusie van antwoord, die aldus in beginsel uiterlijk zes weken na de roldatum zal moeten worden genomen;
- ✓ dat gedaagde wordt verzocht zo spoedig mogelijk, uiterlijk tegelijkertijd met het indienen van een conclusie van antwoord, opgave te doen aan de rolrechter van de verhinderdata in verband met het plannen van een comparitie van partijen of pleidooi.

TENEINDE:

te antwoorden op de volgende vorderingen van eisers:

INLEIDING

1. Inzet van deze procedure is een einde te maken aan het gebruik van gegevens betreffende Nederlandse burgers door de Algemene Inlichtingen- en Veiligheidsdienst ("AIVD") en Militaire Inlichtingen- en Veiligheidsdienst ("MIVD") die in strijd met Nederlandse rechtsbeginselen zijn verkregen. Eisers verzoeken de rechtbank bovendien de Staat te gelasten de persoonlijke levenssfeer en communicatievrijheid van haar burgers zoveel mogelijk te beschermen, onder meer door degenen te informeren van wie gegevens door middel van een ongeoorloofde inmenging in hun privéleven zijn verkregen door de Amerikaanse- of andere (buitenlandse) inlichtingendiensten.

2. Aanleiding voor deze procedure vormt het aftappen van het internet- en telefonieverkeer door de Amerikaanse National Security Agency ("NSA") en andere buitenlandse inlichtingendiensten, zoals de Britse Government Communications Headquarters ("GHCQ"). Recent is bekend geworden dat de NSA alleen al in één maand gegevens van 1,8 miljoen telefoongesprekken heeft afgetapt van Nederlandse ingezetenen. Dit gebeurde in de periode december 2012 - januari 2013.

3. De handelwijze van de NSA (en andere inlichtingendiensten) is in strijd met het Nederlands recht, zo heeft ook de Staat erkend. Terecht heeft Minister Plasterk van Binnenlandse Zaken de spionage- en afluisterpraktijken van onder meer de Amerikanen veroordeeld.

4. Tegelijkertijd profiteren de AIVD en MIVD van deze ongeoorloofde handelwijze door gegevens met de NSA en andere diensten uit te wisselen. Nederland maakt onderdeel uit van een selectieve groep van negen landen, de zogeheten "Nine Eyes", waar intensief mee wordt samengewerkt en informatie mee wordt uitgewisseld. Tot die landen behoren onder meer de

Verenigde Staten en het Verenigd Koninkrijk.[1] Zo komen gegevens die onrechtmatig, want in strijd met het Nederlandse recht en internationale verdragsverplichtingen, zijn verkregen alsnog in handen van Nederlandse inlichtingendiensten. Deze gegevens kunnen vervolgens worden aangewend voor eigen onderzoek.

5. De Ministers van Binnenlandse Zaken en Defensie hebben deze praktijk bevestigd naar aanleiding van Kamervragen. Door het op deze wijze "witwassen" van data die illegaal is verkregen, schendt de Nederlandse Staat de persoonlijke levenssfeer en communicatievrijheid van haar burgers, evenzeer als de Amerikanen dat doen.

6. De Staat mag de grondrechten van haar burgers niet schenden, dat spreekt voor zich. Daarenboven is de Staat verplicht actief maatregelen te treffen om de persoonlijke levenssfeer en de vrijheid om onbespied te communiceren van haar burgers te beschermen. Dat kan de Staat onder meer doen door degenen te informeren van wie data door de NSA en andere inlichtingendiensten is verkregen in strijd met het Nederlands recht.

PROCESPARTIJEN

7. Eisers in deze procedure hebben allemaal een bijzonder belang om zich tegen de praktijken van de NSA en andere buitenlandse inlichtingendiensten te verzetten.

8. Nooitgedagt is strafrechtadvocaat. Tot zijn cliënten behoren uit de aard van zijn praktijk verdachten van strafbare feiten. Hij staat bovendien met grote regelmaat verdachten van (internationaal) terrorisme bij. Nooitgedagt rekent onder andere Amerikaanse verdachten tot zijn cliënten. Hij behandelt regelmatig uitleveringszaken, onder meer van verdachten van Nederland naar de VS. Het belang van advocaten om vrij en vertrouwelijk te communiceren vindt onder meer bescherming in de artikelen 6 en 8 van het EVRM. De Nederlandse Orde van Advocaten voorziet in een systeem van nummerherkenning om te waarborgen dat telefoons van advocaten niet worden afgetapt. Nooitgedagt heeft zijn nummers hiervoor aangemeld.

9. De Winter, een bekende onderzoeksjournalist, is in 2011 verkozen tot journalist van het jaar. Hij vergaarde internationale erkenning door zijn publicaties over databeveiliging en- veiligheid, met name bij de overheid. Hij behandelt overwegend politiek gevoelige onderwerpen waar maatschappelijk debat over is. Zijn bronnen bestaan onder anderen uit personen die zwakheden in databeveiliging blootleggen. Hij communiceert met deze en andere personen via e-mail en telefoon. Om zijn vitale rol als journalist, als publieke waakhond, te waarborgen moet De Winter

[1] De Volkskrant maandag 4 november 2013, 'Profiel: Hoe werkt de National Security Agency? Elektronische alleseter met een verbijsterende vraatzucht', p. 6-7.

in vrijheid kunnen communiceren, verschoond van (buitenlandse) inlichtingendiensten die meeluisteren of gegevens van zijn datacommunicatie aftappen. Slechts wanneer hij de anonimiteit van zijn bronnen kan beschermen, kan hij immers gebruik maken van zijn recht op vrije nieuwsgaring.

10. Van Beek is adviseur informatiebeveiliging, verbonden aan Dexlab. Om de beveiliging van gevoelige systemen te controleren wordt hij door zijn klanten gevraagd om in te breken op hun systemen. Daarnaast voert Van Beek onderzoek uit op het gebied van dataveiligheid en –beveiliging. De doelsystemen zijn vaak eigendom van Amerikaanse bedrijven en bevinden zich dikwijls op Amerikaans grondgebied. Op grond hiervan is het mogelijk dat Van Beek door de Amerikaanse opsporingsautoriteiten wordt aangemerkt als verdachte. Van Beek bezoekt de VS regelmatig.

11. Gonggrijp is een bekende Nederlandse hacker die zich inzet voor transparantie van overheden. Hij is onder meer betrokken geweest bij de initiatieven van de organisatie WikiLeaks om vertrouwelijke documenten van de Amerikaanse overheid te publiceren. In dat kader is hij onderwerp van onderzoek van Amerikaanse opsporingsautoriteiten. Bij het sociale communicatienetwerk Twitter werden de door hem gebruikte IP-adressen opgevraagd. Aannemelijk is dat de NSA en andere inlichtingendiensten ook internet- en telefonieverkeer van Gonggrijp hebben afgetapt. Gonggrijp belt en mailt regelmatig met personen in de VS.

12. Paapst is als onderzoeker en docent verbonden aan de Rijksuniversiteit Groningen, de rechtenfaculteit aldaar. Hij is onder meer gespecialiseerd in de toepassing van het recht op IT-systemen. In zijn onderzoek richt hij zich op internetgovernance, de wijze waarop het internet wordt gereguleerd. De macht van de Amerikaanse regering is in dat kader onderwerp van discussie. Naar aanleiding van de onthullingen over de praktijken van de NSA hebben onder andere de Braziliaanse regering en de directeur van de Internet Corporation for Assigned Names and Numbers (ICANN) zich uitgesproken tegen een grote rol van de VS bij de regulering van het internet. De bescherming van mensenrechten op het internet is daarbij een belangrijk thema. Paapst heeft zich in zijn publicaties kritisch uitgelaten over de Amerikanen, en communiceert hierover regelmatig vertrouwelijk via de e-mail met andere wetenschappers in binnen- en buitenland.

13. Bij de NVSA zijn bijna alle in Nederland gespecialiseerde strafrechtadvocaten aangesloten. De NVSA stelt zich onder meer ten doel datgene te doen dat “voor een goed functioneren van een verdediging in strafzaken dienstig is; en zonodig daartoe in rechte op te treden”.

14. De NVJ stelt zich blijkens haar statuten onder meer tot doel: “nationaal en internationaal te waken en waar nodig te strijden voor de persvrijheid en het recht op informatie van de burgers,

welke vrijheid en welk recht zij beschouwt als haar wezenlijke grondslagen". De vereniging tracht dat doel te realiseren via alle wettige middelen.

15. De Internet Society Nederland is de Nederlandse tak van de in 1992 opgerichte Internet Society, de ISOC. De ISOC is de moederorganisatie achter internationale organen als de Internet Engineering Task Force (IETF), Interactive Advertising Bureau (IAB) en (Internet Research Task Force) IRTF en heeft ruim 44.000 leden verspreid over 170 landen. In Nederland brengt de Internet Society Nederland professionals samen uit onder meer de internetsector, het bedrijfsleven, de overheid, consumentenorganisaties, de not-for-profit-sector, de techniek en het financiële, juridische en academische veld. Net als haar moederorganisatie maakt de Internet Society Nederland zich sterk voor een open, integer en veilig internet voor iedereen.

16. Privacy First, opgericht op 26 maart 2008, heeft blijkens haar statuten ten doel: "het behouden en bevorderen van het recht op privacy, alsmede de persoonlijke vrijheid van leefomgeving, op welke wijze dan ook, onder meer door het in rechte optreden voor alle burgers in Nederland ter bescherming van dit algemene belang en voorts al hetgeen met een en ander rechtstreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de ruimste zin van het woord."

17. Overigens heeft het EHRM aanvaard dat, in een zaak als deze, een vordering op grond van artikel 8 of 10 EVRM ook in het algemeen belang kan worden ingesteld, zelfs als een individueel procesbelang zou ontbreken. [2]

FEITELIJK KADER

De Snowden-onthullingen

18. Op 6 juni 2013 wordt bekend dat de inlichtingendienst NSA op grote schaal internet- en telefonieverkeer van niet-Amerikaanse burgers aftapt. Op die dag onthult klokkenluider Edward Snowden een aantal *top secret* NSA-documenten via The Guardian en The Washington Post die onder meer het controversiële PRISM-programma beschrijven.[3] PRISM is een geheim programma dat door de NSA wordt gebruikt om inlichtingen (o.a. metadata) te vergaren over mensen buiten de Verenigde Staten uit gegevens van negen grote Amerikaanse internetbedrijven, door de NSA ook wel aangeduid als "PRISM providers". Het betreft achtereenvolgens Google, Yahoo!, Facebook, Skype, Apple, Youtube, Microsoft, Paltalk en AOL messenger. De NSA heeft rechtstreeks toegang tot de servers van deze bedrijven.

[2] EHRM 18 mei 2010 (*Kenedy/United Kingdom*), r.o. 119.
[3] http://www.theguardian.com/world/2013/jun/06/us-tech-giants nsa-data.

19. Volgens de Amerikaanse regering wordt PRISM gebruikt ter uitvoering van Section 702 van de FISA (Foreign Intelligence Surveillance Act) Amendment Act (FAA), een wet die het "targeten" van "persons outside the United States" toestaat voor periodes van telkens een jaar.[4] Goedkeuring wordt verkregen bij geheime FISA Courts. Volgens The Guardian, die spreekt van "one-paragraph orders", hebben dergelijke goedkeuringen weinig om het lijf.[5]

20. Omdat een groot deel van het wereldwijde internetverkeer loopt via servers in de Verenigde Staten (zelfs als geen van de communicerende partijen zich in de Verenigde Staten bevindt), is het bereik van PRISM enorm. Volgens Glenn Greenwald, de Guardian-journalist aan wie Snowden de NSA-documenten verstrekte, zijn al meer dan 77.000 "intelligence reports" voortgekomen uit PRISM:

> *When the NSA reviews a communication it believes merits further investigation, it issues what it calls a "report". According to the NSA, "over 2,000 Prism-based reports" are now issued every month. There were 24,005 in 2012, a 27% increase on the previous year. In total, more than 77,000 intelligence reports have cited the PRISM program.*[6]

21. Latere onthullingen maken duidelijk dat de Amerikanen– onder het mom van "*the fight against terrorism*"– niet alleen op grote schaal het telefoon- en internetverkeer tussen burgers registreren dat via Amerikaanse centrales of Amerikaanse servers verloopt, maar ook gegevens opvissen uit glasvezelkabels, om die later te analyseren. De NSA maakt daarvoor, naast PRISM, gebruik van allerlei andere geheime programma's, onder meer "Boundless Informant", "Upstream" en "Xkeyscore".

22. De Snowden-documenten maken verder duidelijk dat niet alleen burgers, maar ook politici, regeringsleiders, de Paus en Secretaris-Generaal van de Verenigde Naties Ban Ki-moon het voorwerp zijn van de afluisterpraktijken. Ook bedrijven worden afgeluisterd. Hieruit blijkt wel dat de taps niet alleen maar nationale veiligheidsdoeleinden dienen, zoals de Amerikanen wel doen voorkomen, maar ook worden aangewend voor diplomatieke- en economische spionage. Dat er ook economische belangen mee gemoeid zijn, blijkt wel uit het bespioneren van Braziliaanse staatsoliebedrijf Petrobas door de NSA.[7]

---

[4] 50 U.S.C. §1881a.
[5] http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant.
[6] http://www.theguardian.com/world/2013/jun/06/us-tech-giants nsa-data.
[7] http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras.

23. Inmiddels weten we dat de Britse veiligheids-en inlichtingendienst, de GHCQ, zich net als de Amerikanen schuldig maakt aan grootschalige afluisterpraktijken. De Britten maken daarbij gebruik van een vergelijkbaar surveillance-programma, Tempora genaamd.[8]

24. Dat ook Nederlandse burgers getroffen worden door de praktijken van de NSA, bleek aan aantal weken geleden, toen bekend werd dat de NSA in één maand tijd 1.8 miljoen Nederlandse telefoongesprekken had onderschept.[9] Minister Plasterk heeft dit vorige week in Nieuwsuur bevestigd.[10]

25. Het onderscheppen, afluisteren, aftappen, registreren, monitoren en opslaan van de communicatie betreffende burgers raakt direct het recht op respect voor het privéleven, zoals onder meer neergelegd in artikel 8 EVRM, artikel 7 en 8 van het Handvest van de Grondrechten van de Europese Unie (hierna: "Handvest") en in artikel 17 International verdrag inzake burgerrechten en politieke rechten (hierna: "IVBPR"). Ook de informatie- en communicatievrijheid, beschermd door artikel 10 EVRM, artikel 11 Handvest en artikel 19 IVBPR, wordt geraakt door de afluisterpraktijken. Het Europees Hof voor de Rechten van de Mens (hierna: "EHRM") heeft in zijn rechtspraak door de jaren heen duidelijke eisen geformuleerd waaraan afluister- en meer algemene surveilleringsmiddellen moeten voldoen, willen zij geoorloofd zijn. Het optreden van de Amerikaanse- en Britse veiligheidsdiensten is echter in flagrante strijd met die vereisten.

26. De afluisterpraktijken van de NSA en hebben wereldwijd geleid tot veel commotie. Duitsland en Frankrijk reageerden verontwaardigd op het afluisterschandaal, en eisen opheldering van de Amerikanen. De Braziliaanse president was woedend en stelde een bezoek aan het Witte Huis tot nader order uit.

27. De verontwaardiging van de Nederlandse Staat over de afluisterpraktijken is, tot dusver, betrekkelijk mild. Dit heeft mogelijk te maken met de hierboven al genoemde intensieve samenwerking van Nederland met andere diensten in het kader van de "Nine Eyes". Het betreft een besloten netwerk bestaande uit de Verenigde Staten, het Verenigd Koninkrijk, Canada, Australië en Nieuw-Zeeland (de "Five Eyes"), uitgebreid met Frankrijk, Nederland, Denemarken en Noorwegen. Een volgend niveau zijn de zogenaamde "14 Eyes" en Nacsi, waarin 26 NAVO-lidstaten zijn betrokken.[11]

---

[8] http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

[9] http://tweakers.net/nieuws/92067/nsa-onderschepte-in-maand-metadata-1-komma-8-miljoen-telefoontjes-in-nederland.html.

[10] http://tweakers.net/nieuws/92297/minister-plasterk-bevestigt-onderscheppen-1-komma-8-miljoen-telefoontjes-door-nsa.html.

[11] *De Volkskrant* maandag 4 november 2013, 'Profiel: Hoe werkt de National Security Agency? Elektronische alleseter met een verbijsterende vraatzucht', p. 6-7. Zie ook http://www.nrc.nl/nieuws/2013/11/01/britten-

28. Begin november werd in de media bericht over het feit dat de Britse GHCQ de Nederlandse AIVD zou adviseren over hoe ze in de toekomst op grote schaal internetverkeer zouden kunnen onderscheppen. Enkel "wettelijke beperkingen" zouden de Nederlandse diensten verhinderen om deze technieken – die neerkomen op het onderscheppen van bulkdata op internet - nu al toe te passen.[12]

29. Het bovenstaande betreft mogelijk het spreekwoordelijke puntje van de ijsberg. Journalist Glenn Greenwald heeft aangekondigd "veel materiaal" over Nederland te hebben, waar hij later inhoudelijk op in zal gaan.

> *De onthullingen over Nederland komen binnenkort. [....] Jullie hebben nog geen idee van de omvang van de Amerikaanse spionage in Nederland*.[13]

Nederland

30. Na de onthullingen van Edward Snowden worden in de Tweede Kamer vragen gesteld over de handelwijze van de NSA en de rol van de Nederlandse Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en/of Militaire Inlichtingen- en Veiligheidsdienst (MIVD) daarbij. Uit de antwoorden van de diverse bewindspersonen blijkt dat de AIVD en MIVD gegevens verkrijgen en gebruiken die via PRISM en vergelijkbare illegale programma's zijn afgetapt.

31. Op 7 juni 2013, een dag na de eerste onthullingen van Snowden, spreekt Minister Ronald Plasterk (hierna: "Minister Plasterk") van Binnenlandse Zaken en Koninkrijksrelaties (hierna: "Binnenlandse Zaken") zich uit tegen de handelwijze van de Amerikaanse NSA, door hem omschreven als het "rondshoppen op het internet".

> *Als de Amerikanen het zonder goede reden doen, is dat in strijd met de bescherming van de privacy en dan is het goed dat het in Europees verband aangekaart wordt*.

32. Hij geeft tegenover de NOS ook aan dat een dergelijk afluisteren "in den brede" in Nederland "totaal in strijd met de wet" zou zijn.[14]

---

adviseerden-aivd-en-mivd-over-afluisteren/ en http://www.volkskrant.nl/vk/nl/13524/De-afluisterpraktijken-van-de-NSA/article/detail/3538122/2013/11/03/Duitsland-spionagediensten-wisselen-kennis-uit.dhtml.

[12] http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden en http://www.nrc.nl/nieuws/2013/11/01/britten-adviseerden-aivd-en-mivd-over-afluisteren/.

[13] http://www.volkskrant.nl/vk/nl/13524/De-afluisterpraktijken-van-de-NSA/article/detail/3524704/2013/10/10/Jullie-hebben-geen-idee-van-omvang-Amerikaanse-spionage-in-Nederland.dhtml.

[14] http://nos.nl/artikel/515409-plasterk-opheldering-spionage-vs.html en http://nos.nl/audio/515485-plasterk-privacy-is-een-grondrecht.html.

33. Op 11 juni 2013 worden kritische Kamervragen gesteld aan minister Opstelten van Justitie,[15] mede naar aanleiding van berichtgeving in De Telegraaf dat ook de AIVD het programma PRISM zou gebruiken (hetgeen door de Ministers van Binnenlandse Zaken en Defensie altijd is ontkend).[16] Kamerlid Gerard Schouw (D66) wil van het kabinet de garantie dat de Nederlandse overheid geen gebruikt maakt van PRISM. Gevraagd wordt ook of de Amerikaanse diensten onbeperkt toegang hebben tot het dataverkeer in Nederland en of de Nederlandse regering weet dat de Amerikaanse overheid programma's op ons loslaat zoals PRISM. Verder wil Schouw weten hoe wordt voorkomen dat door middel van samenwerking tussen Nederland en de Verenigde Staten de lichtere wetgeving in de Verenigde Staten de Nederlandse wet ondermijnt. Verzocht wordt ten slotte om de Amerikanen ter verantwoording te roepen.

34. Minister Opstelten geeft enigszins ontwijkende antwoorden, maar geeft wel aan dat de Nederlandse diensten – net als de Amerikanen, aldus Opstelten – altijd binnen de kaders van de wet werken. Over de manier van samenwerking met buitenlandse diensten doet hij echter geen uitspraken.

> *Dat daarbij* [onderzoek naar strafbare feiten en terroristen] *gebruik wordt gemaakt van moderne technieken is niet alleen vanzelfsprekend, maar ook noodzakelijk. Het verbaast mij dan ook niet dat de Verenigde Staten zich bij hun inlichtingenvergaring ook lijken te richten op het internet en het berichtenverkeer. Het spreekt voor zich dat de inzet van dit soort middelen altijd zorgvuldig, proportioneel en effectief moet zijn. Dat zeg ik met nadruk. De wettelijke waarborgen op het gebied van bescherming van persoonsgegevens en de persoonlijke levenssfeer zijn daarbij evident. Zoals bekend hebben wij in Nederland heldere wettelijke kaders voor onze inlichtingendiensten. Een onafhankelijke commissie houdt toezicht op de exacte werkwijze van onze eigen inlichtingendiensten. Over de exacte werkwijze van onze eigen inlichtingendiensten doen we uiteraard geen mededelingen, ook niet in relatie tot de samenwerking met buitenlandse diensten*.[17] (onderstrepingen advocaat)

35. In een brief van 21 juni 2013 gaat Minister Plasterk nader in op de vraag hoe de wettelijke bevoegdheden van de Nederlandse inlichtingen- en veiligheidsdiensten zich verhouden tot het PRISM-programma of vergelijkbare methoden van informatievergaring. Minister Plasterk bevestigt dat de Nederlandse diensten PRISM niet gebruiken, maar geeft aan dat de Nederlandse overheid wel gegevens met de Amerikanen kan uitwisselen. Minister Plasterk sluit

[15] *Handelingen II* 2012/13, TK 94-5-5. Vragen van het lid Schouw aan de minister van Veiligheid en Justitie over het bericht dat de VS toegang heeft tot alle data (inclusief foto's, e-mails en chatberichten) van grote internetbedrijven als Google, Facebook en Microsoft.
[16] http://www.telegraaf.nl/binnenland/21638965/__Ook_AIVD_bespiedt_online__.html.
[17] *Handelingen II* 2012/13, TK 93-4-5.

in zijn brief niet uit dat gegevens die door andere diensten uit PRISM zijn gewonnen, door Nederlandse inlichtingendiensten worden gebruikt.

> *De AIVD en de MIVD gebruiken het computerprogramma PRISM niet. De AIVD en de MIVD hebben geen onbelemmerde, onbeperkte toegang tot het internetverkeer en het mobiele telefoonverkeer, ook niet via buitenlandse inlichtingen- en veiligheidsdiensten. In het kader van de samenwerking met diensten in andere landen kunnen de AIVD en de MIVD wel gegevens uitwisselen. Artikel 59 van de Wiv 2002 beschrijft de kaders hiervoor. […] Het is de AIVD en de MIVD niet toegestaan diensten in andere landen verzoeken te doen die op grond van de Wiv 2002 niet zijn toegestaan. Het is overigens niet gebruikelijk dat diensten elkaar op de hoogte stellen van de eigen bronnen en de modus operandi. De wijze waarop specifieke gegevens zijn verkregen, wordt doorgaans niet gedeeld.*[18]
> (onderstrepingen advocaat)

36. In zijn latere brief van 3 juli 2013 herhaalt Minister Plasterk dat de AIVD en MIVD veel samenwerken met internationale inlichtingen- en veiligheidsdiensten, maar dat over de vorm van samenwerking geen mededelingen worden gedaan. Plasterk geeft opnieuw aan dat de AIVD en MIVD niet bevoegd zijn om *verzoeken* te doen aan buitenlandse collega-diensten om activiteiten uit te voeren die de Wet op de inlichtingen- en veiligheidsdiensten niet toestaat. Over het *ontvangen* (zonder daartoe strekkend verzoek) wordt echter niks gezegd.[19]

37. Tijdens het Algemeen Overleg van de vaste commissie voor Defensie op 3 juli wordt een aantal zeer kritische vragen gesteld aan Minister Hennis-Plasschaert van Defensie.[20]

> *Kan de Minister ingaan op de vraag of de MIVD gebruikmaakt van gegevens verzameld via PRISM? Wat vindt zij ervan als op deze manier gegevens over Nederlandse burgers worden verzameld, zonder dat er wettelijk toezicht is? Ziet de Minister mogelijkheden om de grondrechten van de Nederlandse burgers te beschermen, aangezien het erop lijkt dat dit niet afgedekt wordt in de Nederlandse wet? […] Zijn er op dit moment expliciete regels en protocollen voor de uitwisseling van gegevens van Nederlandse staatsburgers met buitenlandse veiligheidsdiensten*?[21]

38. Waarop de Minister van Defensie onomwonden antwoordt dat zij niet kan uitsluiten dat de Nederlandse overheid ooit gebruik maakt van gegevens die via PRISM zijn verkregen, noch dat Nederlandse burgers het slachtoffer van PRISM zijn geweest.

---

[18] *Kamerstukken II* 2012/13, 30 977, nr. 56, p. 2.
[19] *Kamerstukken II* 2012/13 30 977, nr. 59.
[20] *Kamerstukken II* 2012/13, 29 924, nr. 100.
[21] *Kamerstukken II* 2012/13, 29 924, nr. 100, p. 8.

Ronald Plasterk heeft mede namens mij en anderen eerder gesteld dat de AIVD en de MIVD niet op de hoogte waren van het programma PRISM als zodanig. Hiermee vertel ik niets nieuws. Wij hebben toen ook meteen gezegd dat de vraag over inlichtingen die mede op basis van informatie uit het PRISM-programma tot stand zijn gekomen, niet te beantwoorden is, omdat het uitwisselen van gegevens tussen diensten zonder bronvermelding plaatsvindt. Dat is de wereld van de diensten. Zo werken zij. Dat is de realiteit. […] Had ik op de hoogte kunnen zijn van het programma PRISM? Het antwoord op die vraag is «nee». Kan ik uitsluiten dat er ooit wordt gebruikgemaakt van gegevens die via het programma PRISM bij onze diensten zijn beland? Het antwoord op die vraag is ook «nee».[22]

Zoals ik net al zei, is het vaak niet bekend op welke wijze die informatie van een andere inlichtingen- en veiligheidsdienst is verkregen. Kortom, ik kan niet uitsluiten dat ook wij een keer over informatie hebben beschikt die misschien wel tot stand is gekomen met dank aan het PRISM-programma. Ik zeg hier gelijk bij dat het wel duidelijk moet zijn dat de MIVD op grond van de Wiv 2002 niet bevoegd is om verzoeken aan buitenlandse collega-diensten te doen tot vergaring van gegevens via methodieken waarover de MIVD volgens de Wiv 2002 zelf niet beschikt. Dit is een belangrijke opmerking. Buitenlandse inlichtingen- en veiligheidsdiensten bepalen daarnaast zelf op basis van de eigen nationale wetgeving – zo werkt het – en het juridische kader welke informatie zij mogen of kunnen delen met andere diensten, bijvoorbeeld de Nederlandse. Dan wordt natuurlijk snel de vraag gesteld of Nederlanders doelwit of slachtoffer van het PRISM-programma zijn geweest. Het probleem is dat ook ik nog over te weinig informatie beschik. De gesprekken tussen de lidstaten van de Europese Unie, waaronder Nederland, en Amerika zijn in volle gang. Ik heb in dit verband ook mijn vragen. […] Hoe verhoudt het PRISM-programma zich tot de Amerikaanse wet? Dat kan ik wel een beetje zeggen, maar dit hebben de leden ook al in de factsheets gelezen. Als een persoon gebruikmaakt van Amerikaanse aanbieders van communicatiediensten, denk aan Facebook, Google et cetera, worden de gegevens verwerkt door een bedrijf dat valt binnen de reikwijdte van de Amerikaanse wetgeving. De verwerking van gegevens van Nederlandse burgers en organisaties valt daarmee onder de Amerikaanse wetgeving. […] Het is niet aan de Nederlandse regering om te beoordelen of de Amerikaanse regering zich aan de Amerikaanse wet houdt. Nederland moet ervan uit kunnen gaan dat de collega-diensten waarmee onze diensten samenwerken, zich aan de eigen wet- en regelgeving houden.[23]

[22] *Kamerstukken II* 2012/13, 29 924, nr. 100, p. 21
[23] *Kamerstukken II* 2012/13, 29 924, nr. 100, p. 24.

Heeft de MIVD een programma zoals PRISM? In eerste instantie zeg ik «nee». Dat is mijn primaire reactie. Ik moet echter gelijk benadrukken dat het nog onduidelijk is wat het programma PRISM nu precies behelst en bevat en onder welke voorwaarden. Voor de rest is het een feit dat wij werken conform de Wiv. Daar staat letterlijk in gespeld wat onze diensten wel en niet mogen.[24]

39. De Minister van Defensie bevestigt dus dat Nederlandse burgers zijn onderworpen aan obscure Amerikaanse wetgeving, zonder dat de Nederlandse overheid maatregelen treft, bijvoorbeeld door afspraken met de Amerikanen, om de privacy van haar burgers te beschermen.

Tussen de inlichtingendiensten zijn er geen openbare overeenkomsten, waarin desnoods over aanvullende voorwaarden wordt geschreven. Ik hoop dat er sprake is van reciprociteit. Daar zet ik zelf ook altijd op in.[25]

40. In de officiële, kabinetsbrede reactie op de onthullingen van Snowden, die volgt op 13 september 2013, lijkt het kabinet de ernst van de zaak te bagatelliseren. Het benadrukt zelfs de positieve kant: de Verenigde Staten hebben beloofd de EU nader te zullen informeren over de spionageprogramma's. Het kabinet schrijft verder dat het de huidige discussies in het Amerikaanse Congres over transparantie "bemoedigend" vindt en de aangekondigde verbeteringen "verheugend". Het kabinet informeert de Tweede Kamer verder over het inmiddels gestarte onderzoek van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten ("CTIVD") naar de gegevensverwerking van de AIVD en de MIVD op het gebied van telecommunicatie,[26] evenals over de ingestelde EU-VS expertgroep.[27]

41. Ook tijdens het algemeen overleg over de onthullingen van Snowden, dat op 16 oktober plaatsvindt,[28] is de reactie van het kabinet mild. Plasterk benadrukt zelfs de waardevolle relatie met bondgenoot Amerika, al spreekt hij wel van een "asymmetrische" toepassing van afluistermethoden door de Amerikanen. Plasterk geeft aan bilaterale afspraken met de Amerikanen te willen onderzoeken.

42. De gematigde, haast passieve reactie van de Nederlandse regering wordt goed weergegeven door de Eerste Kamercommissie voor Immigratie & Asiel/JBZ-Raad en voor Veiligheid en Justitie, in

[24] *Kamerstukken II* 2012/13, 29 924, nr. 100, p. 25.
[25] *Kamerstukken II* 2012/13, 29 924, nr. 100, p. 26.
[26] http://www.ctivd.nl/?Lopende_onderzoeken.
[27] *Kamerstukken II* 2012/13, 30 977, nr. 61.
[28] Conceptverslag van een algemeen over: aftappen gegevens d.d. 16 oktober 2013, te vinden op http://tweedekamer.nl/downloads/document/index.jsp?id=8498fd82-0602-4b50-ad22-8a7dc033070c&title=concept%20overslag%20Aftappen%20gegevens%20in%20Nederland.doc.

haar verslag van 3 oktober 2013, en door de heer Schouw, tijdens het algemeen overleg op 16 oktober.

> *De onthullingen van de heer Snowden betekenen, als ze op waarheid berusten, dat al vele jaren de meest vergaande en ongelegitimeerde inbreuken op de privacy hebben plaatsgevonden, maar ze hebben bij de Nederlandse regering een ontspannen, haast berustend te noemen reactie opgeleverd. Is de regering van mening dat het geen zin heeft om zelfstandig, ook buiten EU-verband, bij onze NAVO-bondgenoot te protesteren of althans om opheldering te vragen? Er zijn ambassadeurs om minder bij de regering ontboden. Hoe beoordeelt de regering de onthulling dat ook diplomaten zijn afgeluisterd? Is een dergelijke handelwijze te rijmen met de bondgenootschappelijke verhoudingen in de NAVO? Wat heeft een papieren waarborg van de privacy van burgers voor zin als de regering, alleen of in EU-verband, niet optreedt tegen de meest ernstige schendingen van de privacy?*[29]
>
> *Als we kijken naar de inzet van de Nederlandse regering tot nu toe, kan de conclusie geen andere zijn dan dat het oorverdovend stil is. Dat haal ik ook uit de brief die de minister op dit punt aan de Kamer heeft gestuurd. Daarin schrijft minister Plasterk dat de discussie in het Amerikaanse Congress bemoedigend en zelfs verheugend is. En dat is het dan ook. Er staat geen oordeel van de Nederlandse regering in de brief, eigenlijk ook geen informatie noch een gevoel van urgentie met betrekking tot het beschermen van grondrechten van Nederlandse burgers. En daar hebben we het hier natuurlijk over.*[30]

43. Uit het voorgaande kunnen, voor wat betreft Nederland, een aantal conclusies worden getrokken:

- Volgens de Ministers van Defensie en Binnenlandse Zaken zijn de afluisterpraktijken van de NSA in ieder geval in strijd met het recht op bescherming van de persoonlijke levenssfeer.
- De Nederlandse AIVD en MIVD maken volgens het kabinet geen gebruik van PRISM (of vergelijkbare programma's). Elke gegevensverwerking door deze diensten geschiedt volgens het kabinet in overeenstemming met de Wet op de inlichtingen- en veiligheidsdiensten.
- De Nederlandse diensten wisselen wel gegevens uit met buitenlandse inlichtingen- en veiligheidsdiensten. Het gebruik van gegevens die met gebruikmaking van het PRISM-programma verkregen zijn is volgens de Ministers van Binnenlandse Zaken en Defensie

[29] *Kamerstukken I* 2013/14, 33 196, M, p. 5.
[30] Conceptverslag van een algemeen over: aftappen gegevens d.d. 16 oktober 2013 p. 4.

niet uit te sluiten. Of de Staat ook informatie gebruikt die afkomstig is uit bijvoorbeeld de Tempora en/Upstream programma's, is nu nog niet duidelijk.

- Glenn Greenwald heeft aangekondigd dat verdere onthullingen over Nederland volgen.

JURIDISCH KADER

Wet op de inlichtingen- en veiligheidsdiensten 2002

44. De Wet op de inlichtingen- en veiligheidsdiensten 2002 (hierna "Wiv 2002") vormt de wettelijke grondslag voor de activiteiten en bevoegdheden van de AIVD en de MIVD. In de Wiv 2002 is onder meer geregeld onder welke voorwaarden beide diensten (persoons)gegevens mogen verwerken. Zo is een gegevensverwerking slechts toegestaan voor een welbepaald doel en moet deze noodzakelijk zijn voor de uitvoering van de Wiv 2002. Ook moet de verwerking op behoorlijke en zorgvuldige wijze en in overeenstemming met de wet gebeuren (artikel 12 Wiv 2002). Artikel 17 Wiv 2002 bevat de algemene bevoegdheid van diensten om aan een ieder gegevens te vragen.

45. Naast de algemene bevoegdheid tot het verwerven van gegevens kunnen de diensten voor hun taakuitvoering een aantal bijzondere bevoegdheden inzetten (artikel 18 e.v. Wiv 2002), waaronder het gericht aftappen en afluisteren van (tele)communicatie (artikel 25 lid 1 Wiv 2002) en het opvragen van verkeersgegevens (artikel 28 lid 1). Omdat de inzet van deze bevoegdheden een beperking vormt van het recht op bescherming van de persoonlijke levenssfeer, zijn deze aan voorwaarden gebonden. Zo mogen deze bevoegdheden slechts worden uitgeoefend voor zover dat noodzakelijk is ter bescherming van de nationale veiligheid (artikel 6 en 7 Wiv 2002) en indien toestemming van de Minister is verkregen, welke toestemming in beginsel wordt verleend voor een duur van drie maanden (Artikel 18 jo. 19 Wiv 2002).

46. De samenwerking tussen de AIVD en de MIVD en buitenlandse inlichtingen- en veiligheidsdiensten wordt beheerst door artikel 59 Wiv 2002. Volgens lid 1 van dat artikel dragen de hoofden van de AIVD en MIVD zorg voor het "onderhouden van verbindingen" met daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen. Lid 2 en 4 maken ten aanzien van deze samenwerking onderscheid tussen het *verstrekken* van gegevens respectievelijk het verlenen van (technische) *ondersteuning* aan buitenlandse instanties.

    1. *De hoofden van de diensten dragen zorg voor het <u>onderhouden van verbindingen</u> met daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen.*

2. *In het kader van het onderhouden van verbindingen als bedoeld in het eerste lid kunnen aan deze instanties gegevens worden verstrekt ten behoeve van door deze instanties te behartigen belangen, voor zover:*
   a. *deze belangen niet onverenigbaar zijn met de belangen die de diensten hebben te behartigen, en*
   b. *een goede taakuitvoering door de diensten zich niet tegen verstrekking verzet.*
3. *Op de verstrekking van gegevens als bedoeld in het tweede lid, zijn de artikelen 37, 41 en 42 van overeenkomstige toepassing.*
4. *In het kader van het onderhouden van verbindingen als bedoeld in het eerste lid kunnen voorts op een daartoe strekkend schriftelijk verzoek aan deze instanties technische en andere vormen van ondersteuning worden verleend ten behoeve van door deze instanties te behartigen belangen, voor zover:*
   a. *deze belangen niet onverenigbaar zijn met de belangen die de diensten hebben te behartigen, en*
   b. *een goede taakuitvoering door de diensten zich niet tegen de verlening van de desbetreffende vorm van ondersteuning verzet.*
5. *Een verzoek om ondersteuning als bedoeld in het vierde lid dient ondertekend te zijn door de daartoe bevoegde autoriteit van deze instantie en omvat een nauwkeurige omschrijving van de verlangde vorm van ondersteuning alsmede de reden waarom de ondersteuning wenselijk wordt geacht. De verzochte ondersteuning wordt slechts verleend, indien daarvoor toestemming is verkregen van Onze betrokken Minister.*
6. *Onze betrokken Minister kan de bevoegdheid tot het verlenen van toestemming als bedoeld in het vijfde lid uitsluitend mandateren aan het hoofd van de dienst, voor zover het gaat om verzoeken met een spoedeisend karakter. Van een verleende toestemming door het hoofd van de dienst wordt Onze betrokken Minister terstond geïnformeerd.*

47. Beide vormen van samenwerking mogen volgens deze bepaling slechts plaatsvinden voor zover de door de buitenlandse dienst te behartigen belangen niet onverenigbaar zijn met de belangen die de Nederlandse dienst moet behartigen, en als een goede taakuitvoering door de dienst zich niet tegen samenwerking verzet (lid 2 en lid 4).

48. De AIVD verricht zijn taken in ondergeschiktheid aan de wet. Dit houdt in dat de normen, en zeker ook de grond- en mensenrechten, die zijn neergelegd in de Grondwet en in de internationale verdragen die door Nederland zijn geratificeerd, moeten worden gerekend tot de belangen die de AIVD heeft te behartigen.[31] Ook de toezichthouder, de CTIVD, stelt in haar meest recente toezichtsrapport inzake de samenwerking van de AIVD met buitenlandse inlichtingen- en veiligheidsdiensten buiten twijfel dat deze normen een essentieel onderdeel uit

[31] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 65 en *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 74.

dienen te maken van de besluitvorming omtrent het aangaan en onderhouden van relaties met buitenlandse diensten. Volgens de CTIVD is daarbij eveneens van belang of buitenlandse collega-diensten in verband wordt of is gebracht met schendingen van mensenrechten.[32]

Artikelen 8 en 10 EVRM, artikelen 7, 8 en 11 Handvest

49. Het recht op bescherming van de persoonlijke levenssfeer (privacy) wordt beschermd door artikel 8 EVRM en artikel 7 en 8 van het Handvest (ten behoeve van de leesbaarheid hierna tezamen ook wel aan te duiden als "artikel 8 EVRM"). De vrije nieuwsgaring, waaronder de bescherming van journalistieke bronnen, vindt onder meer bescherming in artikel 10 EVRM en artikel 11 van het Handvest (hierna ook wel "artikel 10 EVRM"). Deze artikelen werken rechtstreeks door in de Nederlandse rechtsorde en maken derhalve onderdeel uit van het Nederlandse recht (artikel 93 jo. 94 Grondwet). De artikelen luiden achtereenvolgens:

Artikel 8 EVRM - Recht op eerbiediging van privéleven, familie- en gezinsleven

1. *Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.*
2. *Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.*

Artikel 7 Handvest - Eerbiediging van het privé-leven en het familie- en gezinsleven

Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.

Artikel 8 Handvest - Bescherming van persoonsgegevens

1. *Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.*
2. *Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet.Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.*

[32] Toezichtsrapport inzake de samenwerking van de AIVD met buitenlandse inlichtingen en/of veiligheidsdiensten, CTIVD nr. 22A, p. 8.

3. *Een onafhankelijke autoriteit ziet toe op de naleving van deze regels.*

Artikel 10 EVRM – Vrijheid van meningsuiting

1. *Een ieder heeft recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te koesteren en de vrijheid om inlichtingen of denkbeelden te ontvangen of te verstrekken, zonder inmenging van enig openbaar gezag en ongeacht grenzen. Dit artikel belet Staten niet radio-omroep-, en bioscoop- of televisieondernemingen te onderwerpen aan een systeem van vergunningen.*
2. *Daar de uitoefening van deze vrijheden plichten en verantwoordelijkheden met zich brengt, kan zij worden onderworpen aan bepaalde formaliteiten, voorwaarden, beperkingen of sancties, die bij de wet zijn voorzien en die in een democratische samenleving noodzakelijk zijn in het belang van de nationale veiligheid, territoriale integriteit of openbare veiligheid, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden, de bescherming van de goede naam of de rechten van anderen, om de verspreiding van vertrouwelijke mededelingen te voorkomen of om het gezag en de onpartijdigheid van de rechterlijke macht te waarborgen.*

Artikel 11 Handvest – Vrijheid van meningsuiting en van informatie

1. *Eenieder heeft recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te koesteren en de vrijheid om inlichtingen of denkbeelden te ontvangen of te verstrekken, zonder inmenging van enig openbaar gezag en ongeacht grenzen.*
2. *De vrijheid en de pluriformiteit van de media worden geëerbiedigd.*

50. Het recht op privacy (artikel 8 EVRM) beschermt een groot aantal facetten van het privéleven, waaronder de woning, het gezinsleven, de eer en goede naam, de communicatie, en persoonsgegevens. Ook verkeersgegevens, ook wel *metadata*[33] genoemd, die niet de inhoud van de communicatie betreffen, maar die informatie geven over bepaalde gegevens (zoals bijvoorbeeld datum, telefoonnummer, tijdstip en plaats), genieten bescherming onder artikel 8 EVRM.[34] Dat is ook niet vreemd: dergelijke ogenschijnlijk neutrale gegevens, bijvoorbeeld over waar en wanneer er met wie is gebeld of gemaild, bevatten dikwijls waardevollere informatie dan wat er wordt gezegd en geschreven.

51. Artikel 10 EVRM, de vrijheid van meningsuiting, beschermt niet alleen de vrijheid om informatie (en meningen) te verspreiden, maar ook het recht om zonder inmenging van enige

[33] President Obama heeft zich ter verdediging van het optreden van de NSA erop beroepen dat er slechts "metadata" worden geregistreerd.
[34] EHRM 2 augustus 1984 (*Malone/UK*), r.o. 84.

openbaar gezag te communiceren en informatie te ontvangen (te garen). Ook de vrijheid van nieuwsgaring van journalisten wordt beschermd door artikel 10 EVRM.

52. Dat het grondrecht op communicatievrijheid, met name ook het recht om informatie te ontvangen, in het geding is als er continu wordt meegekeken (door middel van strategische monitoring) is duidelijk. Het recht op privacy en vrijheid van meningsuiting zijn in dat verband nauw met elkaar verweven, in die zin dat respect voor privacy een noodzakelijke voorwaarde is voor de uitoefening van het recht op informatievrijheid:

> *The right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas. Restrictions of anonymity in communication, for example, have an evident chilling effect on victims of all forms of violence and abuse, who may be reluctant to report for fear of double victimization.*[35]

53. Van het gebruik van surveillance- en afluistermethoden gaat een sterk *chilling effect* uit op de communicatievrijheid, met name voor partijen als journalisten en klokkenluiders, voor wie de communicatievrijheid een noodzakelijke voorwaarde is om hun publieke taak als "public watchdog" te kunnen vervullen.[36]

54. Het EVRM stelt voor elke beperking van het recht op privacy en de vrije nieuwsgaring de eis dat deze is voorzien bij wet ("in accordance with the law"), een legitiem doel dient, en noodzakelijk is in een democratische samenleving (artikel 8 lid 2 en artikel 10 lid 2 EVRM).

<u>Rechtspraak EHRM</u>

55. Het EHRM heeft herhaaldelijk geoordeeld over de toelaatbaarheid van het onderscheppen van communicatie en het toepassen van heimelijke surveillance- en afluistermethoden, zowel in zaken over het individueel monitoren als in zaken over algemeen (strategisch) monitoren.[37]

56. Die rechtspraak maakt duidelijk dat het onderscheppen, registreren en/of afluisteren van de communicatie van burgers – ook indien dit gebeurt door inlichtingen-en veiligheidsdiensten –

---

[35] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, United Nations General Assembly, 17 april 2013, p. 7.

[36] Zie ook het Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, United Nations General Assembly, 17 april 2013, te vinden op http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

[37] EHRM 6 september 1978 (*Klass/ Germany*), EHRM 2 augustus 1984 (*Malone/ UK*), EHRM 24 april 1990 (*Kruslin/ France*), EHRM 29 juni 2006 (*Weber & Saravia*), EHRM 1 juli 2008 (*Liberty/ UK),* EHRM 4 december 2008 (*S. and Marper/ UK*).

slechts onder zeer stringente voorwaarden is toegestaan. Het EHRM hecht daarbij met name sterk aan de aanwezigheid van adequate en effectieve wettelijke waarborgen tegen willekeur. Want, zo overweegt het EHRM, het enkele bestaan van wetgeving en/of praktijk die een systeem van heimelijke surveillance vormen en toestaan, vormt al een inmenging in de uitoefening van het recht op privacy.

> *[T]he mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them.*[38]

57. Daarom eist het EHRM dat de reikwijdte en uitvoeringsmodaliteiten van een wettelijke (afluister- en/of monitor)bevoegdheid voldoende precies zijn aangegeven en dat er procedurele waarborgen zijn vastgelegd, teneinde machtsmisbruik en willekeur te voorkomen. Het EHRM heeft dit herhaaldelijk benadrukt:

> *[…] this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate. The Court must be satisfied that, whatever system is adopted, there exist adequate and effective guarantees against abuse.*[39]

> *Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident. […] Undoubtedly, as the Government rightly suggested, the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. […] Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.*[40]

[38] EHRM 29 juni 2006 (*Weber & Saravia*), r.o. 78, onder verwijzing naar EHRM 6 september 1978 (*Klass/ Germany*), r.o. 41 en EHRM 2 augustus 1984 (*Malone/ UK*), r.o. 64.
[39] EHRM 6 september 1978 (*Klass/ Germany*), r.o. 49.
[40] EHRM 2 augustus 1984 (*Malone/ UK*), r.o. 67.

Above all, the system does not for the time being afford adequate safeguards against various possible abuses. For example, the categories of people liable to have their telephones tapped by judicial order and the nature of the offences which may give rise to such an order are nowhere defined. Nothing obliges a judge to set a limit on the duration of telephone tapping. (...) The information provided by the Government on these various points shows at best the existence of a practice, but a practice lacking the necessary regulatory control in the absence of legislation or case-law.[41]

Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.[42] (onderstrepingen advocaat)

58. In 2006 heeft het EHRM, in een zaak over het onderscheppen van telecommunicatie, zes concrete minimumwaarborgen geformuleerd om te beoordelen of de reikwijdte en uitvoeringsmodaliteiten van een wettelijke bepaling die de grondslag biedt voor afluistermaatregelen voldoende duidelijk zijn. Wil een dergelijke wet voldoen aan de eisen die het EVRM stelt, dan moeten daarin volgens het Hof de *reden/aanleiding* voor de maatregel en de *categorieën van personen* die worden getroffen door de maatregel worden gedefinieerd. Daarnaast moeten de *duur* van de maatregel, de te volgen *procedure*, de te nemen *voorzorgsmaatregelen*, alsmede de *omstandigheden* waaronder de gegevens mogen of moeten worden *vernietigd*, worden vastgelegd.

In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed (see, inter alia, Huvig, cited above, p. 56, § 34; Amann, cited above, § 76; Valenzuela Contreras,

[41] EHRM 24 april 1990 (*Kruslin*), r.o. 35
[42] EHRM 29 juni 2006 (*Weber en Saravia/Duitsland*), r.o. 94.

cited above, pp. 1924-25, § 46; and Prado Bugallo v. Spain, no. 58496/00, § 30, 18 February 2003). [43]

59. Dat deze toetsingsgronden ook gelden voor "more general programs of surveillance" – en dus ook voor algeheel strategisch monitoren– heeft het EHRM bevestigd in het *Liberty*-arrest:

> *It is true that the above requirements were first developed by the Court in connection with measures of surveillance targeted at specific individuals or addresses [...] However, the Weber and Saravia case was itself concerned with generalised "strategic monitoring", rather than the monitoring of individuals [...]. The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other*. [...][44] (onderstreping advocaat)

Schending door de Amerikaanse en Britse inlichtingendiensten

60. Dat de afluisterpraktijken van de Amerikaanse en Britse inlichtingen- en veiligheidsdiensten onverenigbaar zijn met de bescherming van de persoonlijke levenssfeer en de communicatievrijheid, zoals gewaarborgd in artikel 8 EVRM en 10 EVRM is evident (maar ook met vergelijkbare internationale verdragsregels, zoals de artikelen 17 en 19 IVBPR, waaraan ook de Amerikanen gebonden zijn). De wettelijke criteria voor toepassing van de spionagepraktijken door de NSA zijn ontoegankelijk en vaag; de rechterlijke controle is geheim. Dat de abstract geformuleerde FISA Amendments Act geen voldoende wettelijke basis biedt zoals vereist door artikel 8 EVRM en het EHRM, is duidelijk. Daaruit blijkt immers niet onder welke omstandigheden via welke procedure en met welke modaliteiten de Amerikanen afluisterbevoegdheden kunnen inzetten voor het beëindigen van welke categorieën van illegaal gedrag.

61. Daar komt nog bij dat de inzet van afluisterbevoegdheden door deze diensten volstrekt disproportioneel is. Om die reden is ook niet voldaan aan het vereiste dat de beperking noodzakelijk is in een democratische samenleving. De schaal waarop door deze diensten wordt afgeluisterd en geregistreerd is dusdanig, dat er duidelijk een grens is overschreden. Het afluisteren blijft immers niet beperkt tot mensen waarvan vermoed wordt dat zij betrokken zijn bij terrorisme. Er is, daarentegen, sprake van een brede, wereldwijde preventieve controle van gesprekken, e-mails en internetpaden.

---

[43] EHRM 29 juni 2006 (*Weber en Saravia/Duitsland*), r.o. 95. Zie ook de noot van Dommering bij het Liberty-arrest, waarin hij deze toetsingsgronden samenvat; EHRM 1 juli 2008, *NJ* 2010, 325, m. nt. Dommering (*Liberty*).

[44] EHRM 1 juli 2008 (*Liberty*), r.o. 63.

62. Ook Minister Plasterk heeft bevestigd dat een dergelijke werkwijze in Nederland volstrekt in strijd met de wet zou zijn, en dat de balans van de Amerikanen tussen privacy en terrorismebestrijding zoek is.[45]

Schending artikelen 8 en 10 EVRM

63. Ook de Staat schendt artikel 8 en 10 EVRM, door – al dan niet op verzoek - gegevens te ontvangen en gebruiken die door buitenlandse diensten in strijd met artikel 8 en 10 EVRM zijn verkregen. Artikel 59 Wiv, het artikel dat ook volgens de Staat het kader biedt waarbinnen de AIVD en MIVD gegevens mogen uitwisselen met diensten van andere landen,[46] biedt geen – laat staan een voorzienbare – wettelijke basis in de zin van artikel 8 lid 2 EVRM voor het ontvangen en gebruiken van dergelijke gegevens.

64. Artikel 59 Wiv 2002 zwijgt volledig over de mogelijkheid dat via buitenlandse diensten gegevens worden ontvangen, laat staan dat het artikel waarborgen en modaliteiten bevat die aangeven wanneer dat is toegestaan, welke procedure moet worden gevolgd, hoe lang de gegevens mogen worden verzameld en bewaard, onder welke voorwaarden, en welke voorzorgsmaatregelen genomen moeten worden. Artikel 59 spreekt, daarentegen, slechts over het "onderhouden van verbindingen" met buitenlandse diensten, alsmede over het "verstrekken" van informatie en het bieden van "ondersteuning" aan deze diensten. De Wiv 2002 en het ontvangen en gebruiken van data uit programma's als PRISM kan niet de toets doorstaan van de hierboven besproken rechtspraak van het EHRM.[47]

65. Uit de memorie van toelichting bij de Wiv 2002 volgt weliswaar dat de Nederlandse diensten er op grond van artikel 59 ook belang bij kunnen hebben om met betrekking tot een bepaald onderwerp aan een vergelijkbare dienst te *vragen* of zij informatie hebben of aan informatie kunnen komen,[48] maar dergelijke verzoeken (en de eisen waaraan die moeten voldoen) zijn evenmin in de Wiv 2002 geregeld.[49] Deze verzoeken zijn dus– bij gebrek aan waarborgen en procedurele voorschriften – ook niet "voorzien bij wet" zoals bedoeld in artikel 8 lid 2 EVRM.[50] Anders dan geldt voor het loutere ontvangen van gegevens, veronderstelt het vragen overigens een *actieve handeling* (een verzoek) van de Staat.

---

[45] Aldus Plasterk op 30 oktober in Nieuwsuur.
[46] *Kamerstukken II* 2012/13, 30 977, nr. 56, p. 2.
[47] EHRM 29 juni 2006 (*Weber en Saravia/Duitsland*), r.o. 94 en EHRM 1 juli 2008 (*Liberty*), r.o. 63.
[48] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 73.
[49] Toezichtsrapport inzake de samenwerking van de AIVD met buitenlandse inlichtingen en/of veiligheidsdiensten, CTIVD nr. 22A, p. 33.
[50] In het meest recente toezichtsrapport heeft de CTIVD de AIVD ook nadrukkelijk aanbevolen om de procedure voor het doen van verzoeken schriftelijk vast te leggen, p. 34.

66. Over het ontvangen, gebruiken, verzamelen, opslaan, en vernietigen van gegevens via buitenlandse diensten is in de Wiv 2002 dus niks bepaald, terwijl dit – wil een beperking van de privacy geoorloofd zijn – wel zou moeten. Het gevolg hiervan is dat de AIVD en MIVD via buitenlandse diensten mogelijk de beschikking krijgen over gegevens die met ongeoorloofde middelen zijn verkregen. Door dit "witwassen" van illegale data wordt zowel het recht op privacy als onze eigen Nederlandse wetgeving, en de waarborgen die daarin zijn vastgelegd, volledig ondermijnd door de lichtere, obscure en willekeurige wetgeving van de Verenigde Staten.

67. Het is overigens niet voor het eerst dat de conclusie luidt dat de Wiv 2002 niet voldoet aan de kwaliteitseisen die het EVRM stelt. In een zaak van De Telegraaf tegen de Staat – die ging over het afluisteren van journalisten op grond van de Wiv 2002 – oordeelde het EHRM al eens dat de Wiv 2002 niet voldeed aan het voorzienbaarheidsvereiste, omdat niet was voorzien in een onafhankelijke toets voorafgaande aan de inzet van bijzondere bevoegdheden door de AIVD tegen journalisten teneinde hun journalistieke bronnen te achterhalen.[51]

68. Voor de volledigheid zij nog opgemerkt dat de in artikel 1 sub f jo. artikel 12 Wiv 2002 neergelegde, algemene bevoegdheid voor de AIVD en de MIVD om gegevens te verwerken, evenmin een (afdoende) wettelijke basis kan bieden voor het ontvangen van gegevens van buitenlandse inlichtingen- en veiligheidsdiensten. Hetzelfde geldt voor artikel 17 Wiv 2002. Voor al deze artikelen geldt hetzelfde als hetgeen hierboven over artikel 59 Wiv 2002 is opgemerkt.

Schending Wiv 2002

69. Het ontvangen van gegevens door de Staat via buitenlandse diensten die mogelijk mede op basis van ongeoorloofde middelen (zoals PRISM) tot stand zijn gekomen, is niet alleen in strijd met de artikelen 8 en 10 EVRM, maar ook in strijd met de Wiv 2002.

70. Voor zover die gegevens zijn ontvangen na een daartoe strekkend *verzoek* van de Nederlandse AIVD of MIVD geldt dat dit in strijd is met het – door de Ministers Plasterk en Hennis-Plasschaert zelf herhaaldelijk aangehaalde – uitgangspunt dat de Nederlandse overheid uitsluitend om de inzet van bevoegdheden door een buitenlandse dienst mag verzoeken die de Nederlandse overheid zelf ook bezit, met inachtneming van de wettelijke vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit die aan de inzet van die bevoegdheden zijn gesteld.[52] Dat het "uitwisselen van gegevens tussen de diensten zonder bronvermelding"

[51] EHRM 22 november 2012 (*De Telegraaf/Nederland*).

[52] Zie ook Toezichtsrapport inzake de samenwerking van de AIVD met buitenlandse inlichtingen en/of veiligheidsdiensten, CTIVD nr. 22A, p. 33. "*De ondersteuning door een buitenlandse dienst op verzoek van de AIVD vindt immers plaats ten behoeve van de goede taakuitvoering door de AIVD. De AIVD is bij het verrichten van zijn taak gebonden aan de wet (artikel 2 WIV 2002). Een verzoek van de AIVD ten behoeve van*

plaatsvindt, zoals Ministers Plasterk, Opstelten en Hennis-Plasscheart hebben aangegeven, vormt natuurlijk geen rechtvaardiging voor het gebruik van gegevens die onder de Wiv 2002 niet hadden mogen worden verkregen. Integendeel. Wat geldt voor het doen verzoeken om informatie en ondersteuning aan buitenlandse inlichtingen-en veiligheidsdiensten, geldt vanzelfsprekend ook voor het ontvangen van informatie.

71. Bovendien geldt dat – of nu wel of geen verzoek om informatie wordt gedaan – de Nederlandse diensten zijn onderworpen aan de grond- en mensenrechten die zijn neergelegd in de Grondwet en in de internationale verdragen die door Nederland zijn geratificeerd, welke zij tot hun eigen belangen moeten rekenen.[53] Het gebruik van informatie die in strijd met het recht op privacy en de informatievrijheid is verkregen, is dus niet verenigbaar met de belangen die de diensten hebben te behartigen (artikel 59 lid 2 sub a en lid 4 sub a Wiv 2002).

72. Daarom moeten de AIVD en MIVD, voorafgaand aan een eventuele samenwerking met buitenlandse diensten, de grondrechten bij hun afweging betrekken. Een concrete aanwijzing dat informatie afkomstig is van een schending van grondrechten kan daarom – en moet in dit geval – reden zijn om af te zien van het gebruik van informatie afkomstig van een buitenlandse dienst, zo vindt ook de toezichthouder, de CTIVD (die het voorbeeld van foltering noemt):

> *Des te meer is het van belang dat, voorafgaand aan de samenwerking met een buitenlandse inlichtingen- of veiligheidsdienst, zorgvuldig wordt gewogen in hoeverre de mensenrechtensituatie in een land aan samenwerking met de desbetreffende dienst van dat land in de weg staat. Eveneens zal de AIVD zich, naarmate de samenwerkingsrelatie voortduurt dan wel andere vormen aanneemt, telkens dienen af te vragen tot welk niveau de samenwerking met een dergelijke dienst kan strekken en of de intensiteit van de samenwerkingsrelatie niet in strijd is met de belangen die de dienst heeft te behartigen. Ook dient de AIVD alert te zijn op mogelijke neveneffecten bij samenwerking. […] Evenzo geldt dat ingeval de AIVD inderdaad concrete aanwijzingen heeft dat informatie afkomstig van een buitenlandse dienst door marteling is verkregen, de AIVD zal moeten afzien van het gebruik van deze informatie. […]* (onderstrepingen advocaat).
>
> *Eveneens kan zich de situatie voordoen dat er signalen zijn van schendingen van mensenrechten in een land met een lange democratische traditie. […] Per buitenlandse dienst moet door de AIVD een doordachte afweging worden gemaakt, niet alleen bij het*

de eigen taakuitvoering om ondersteuning van een buitenlandse dienst door middel van de inzet van bevoegdheden waartoe de AIVD zelf niet bevoegd is of die niet voldoet aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit, is naar het oordeel van de Commissie onrechtmatig."

[53] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 65.

aangaan van de samenwerkingsrelatie maar ook naargelang een al bestaande samenwerkingsrelatie wordt geïntensiveerd of van karakter verandert.

73. Dat er in het geval van de Amerikaanse en Britse inlichtingendienst "signalen" zijn die erop wijzen dat deze diensten het recht op privacy schenden, is na alle Snowden-onthullingen wel duidelijk.

Conclusie

74. Het uitwisselen van gegevens met de Amerikanen, terwijl aannemelijk is deze gegevens door een schending van het recht op privacy en de informatievrijheid zijn verkregen, is in strijd met de artikelen 8 en 10 EVRM alsmede met de Wiv 2002.

75. Plasterk gaf recent aan nadere afspraken met de Amerikanen te willen maken, om "opnieuw te definiëren" hoe Nederland en de Verenigde Staten met elkaar omgaan.[54] Totdat de Staat daadwerkelijk heldere afspraken heeft gemaakt met de Verenigde Staten en de Amerikanen zich daar ook kenbaar aan houden, is het Nederland simpelweg niet toegestaan om gegevens uit te wisselen met de NSA, in ieder geval niet zolang niet vaststaat dat deze op rechtmatige wijze zijn verkregen.

Positieve verplichting

76. Het is algemeen aanvaard dat artikel 8 EVRM niet alleen een verplichting voor de Staat bevat om zich van inbreuken op de persoonlijke levenssfeer te onthouden (een *negatieve* verplichting), maar ook een *positieve* verplichting voor de Staat om actief maatregelen te nemen om de persoonlijke levenssfeer van haar burgers te beschermen. Hetzelfde geldt voor artikel 10 EVRM ten aanzien van de vrije nieuwsgaring.

77. Het toetsingskader om te beoordelen of de Staat haar positieve verplichting op grond van deze bepalingen heeft geschonden, verschilt niet wezenlijk van de toets die op grond van de tweede leden hiervan moet plaatsvinden.

The Court observes that although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference. In addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private and family life. These obligations may involve the adoption of measures designed to secure respect for private and family life even in the sphere of the relations of individuals between themselves. The boundaries between the State's positive and negative obligations under

[54] Zie onder meer De Volkskrant van 31 oktober 2013: "NSA erkent aftappen Nederland".

Article 8 do not lend themselves to precise definition. The applicable principles are nonetheless similar. In particular, in both instances regard must be had to the fair balance to be struck between the competing interests. [55]

78. Nederland is nog niet zo lang geleden al eens door het EHRM op de vingers getikt, omdat zij onvoldoende had gedaan om identiteitsfraude op haar grondgebied actief te bestrijden. Dat leverde een schending van haar positieve verplichting op grond van artikel 8 EVRM op.[56]

79. Dat de Staat in dit geval tekort schiet in haar positieve verplichting om de burgers te beschermen tegen de Amerikaanse afluisterpraktijken, is evident. Tot op heden blijkt uit niets dat de Staat actie onderneemt om deze flagrante mensenrechtenschendingen door buitenlandse veiligheids- en inlichtingendiensten tot een einde te brengen. Integendeel, de Staat kijkt passief toe en geeft aan de resultaten van de EU-VS expertgroep te willen afwachten.

80. Pas weken nadat de praktijken van de NSA en andere inlichtingendiensten bekend worden, geeft Plasterk aan nadere afspraken met de Amerikanen te willen maken. [57] Dergelijke bilaterale afspraken zijn er voorlopig nog niet en het is onzeker of ze er zullen komen. Pogingen daartoe van onder meer Frankrijk en Duitsland zijn tot op heden tevergeefs gebleken. [58]

81. Dat betekent echter niet dat de Staat er ondertussen niet toe verplicht is om alle mogelijke passende maatregelen te treffen om de persoonlijke levenssfeer en communicatievrijheid van haar burgers zoveel mogelijk te beschermen.

82. Op grond van haar positieve verplichting zou de Staat *in ieder geval* de burgers over wie zij gegevens heeft ontvangen van buitenlandse inlichtingen- en veiligheidsdiensten die in strijd met artikel 8 en 10 EVRM zijn verkregen, daarover moeten informeren. Deze informatieverschaffing zou onder meer moeten zien op de periode, de aard, de hoeveelheid en de doeleinden waarvoor de gegevens zijn verzameld. Daarnaast moet de Staat personen de mogelijkheid bieden om uitsluitsel te verkrijgen over de vraag of gegevens over hem of haar in strijd met artikel 8 en 10 EVRM zijn verkregen. Tot slot moet de Staat ten minste maatregelen nemen om ervoor te zorgen dat door haar ontvangen gegevens via buitenlandse inlichtingen- en veiligheidsdiensten die op ongeoorloofde wijze tot stand zijn gekomen, te wissen.

---

[55] EHRM 4 december 2007 (*Dickson/ UK*).
[56] EHRM 14 februari 2012 (*Romet/ Nederland*)
[57] Zie onder meer De Volkskrant van 31 oktober 2013: “NSA erkent aftappen Nederland”.
[58] Zie ook de motie van de leden Schouw en Pecthold, *Kamerstukken II* 2013/14, 21 501-20, nr. 812, waarin de regering wordt aangespoord om zich aan te sluiten bij het Frans-Duitse initiatief of zelfstandig het gesprek met de Amerikanen aan te gaan.

VERWEREN GEDAAGDE

83. Er zijn eisers geen verweren bekend van de Staat met betrekking tot de vorderingen.

84. In het bovenstaande is uitgebreid ingegaan op de uitlatingen van de Staat in de Tweede Kamer. Voor zover daaruit al enige verweren zouden blijken, is in het bovenstaande reeds genoegzaam aangetoond waarom de Staat in strijd handelt met het Nederlandse recht en internationale verdragsverplichtingen.

VORDERINGEN

85. De vorderingen kunnen als volgt worden toegelicht. De vordering onder I betreft een verklaring voor recht dat de Staat in strijd heeft gehandeld met Nederlands recht en de in het lichaam van de dagvaarding omschreven verdragsrechtelijke bepalingen, in het bijzonder door gegevens te ontvangen of te gebruiken van buitenlandse inlichtingendiensten. Eisers gaan er hierbij vanuit dat deze inlichtingendiensten op hun beurt in strijd hebben gehandeld met de betreffende bepalingen of andere internationale verplichtingen (zoals de artikelen 17 of 19 IVBPR). Eisers hebben belang bij deze verklaring voor recht, onder meer omdat het niet voldoen hieraan door de Staat onrechtmatig handelen jegens hen met zich mee zou brengen.

86. De vordering sub II bevat een op te leggen verbod om nog langer in strijd met, kortweg, de persoonlijke levenssfeer en vrijheid van meningsuiting van eisers te handelen alsmede van degenen wier (gelijksoortige) belangen de betrokken stichtingen en verenigingen behartigen. Deze vordering is mede gebaseerd op art. 3:305a BW. De vordering kan beschouwd worden als een negatieve verplichting, althans een verplichting van de Staat zich van bepaald handelen te onthouden.

87. De vordering onder III betreft een positieve verplichting, namelijk om iets te doen. De vorderingen zijn deels gespecificeerd. Het zijn allemaal waarborgen om de persoonlijke levenssfeer of de vrije nieuwsgaring zoveel mogelijk te beschermen. Hetgeen is opgenomen onder i betreft een verplichting om informatie te verstrekken. Vergelijk in dit verband artikelen 10 en 11 van Privacyrichtlijn (95/46/EG).[59] De vordering onder ii betreft een recht van de betrokkene op toegang tot gegevens betreffende zijn persoon, onder meer gebaseerd op artikel 12 onder a van de Privacyrichtlijn. De last om gegevens te wissen, onder iii, is onder meer gebaseerd op artikel 12 onder b van de Privacyrichtlijn. De termijnen zijn steeds gekozen om de

[59] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Publicatieblad,* Nr. L 281 van 23/11/1995 blz. 0031 - 0050

Staat de mogelijkheid te geven aan de lasten te voldoen, onder meer door overleg met de buitenlandse inlichtingendiensten.

BEVOEGDHEID

88. De Rechtbank Den Haag is te dezer zake bevoegd op grond van artikel 99 Rv.

MITSDIEN:

Het de rechtbank behage bij vonnis, zoveel mogelijk uitvoerbaar bij voorraad:

I. Te verklaren voor recht dat de Staat in strijd handelt met het Nederlands recht, in het bijzonder met de Wiv 2002, en/of internationale verdragsverplichtingen, in het bijzonder artikel 8 EVRM en artikel 7 en/of 8 van het Handvest, en/of artikel 10 EVRM en artikel 11 van het Handvest, door van buitenlandse inlichtingen- en veiligheidsdiensten gegevens te ontvangen en/of te gebruiken die via ongeoorloofde middelen zijn vergaard, zoals met behulp van PRISM of vergelijkbare programma's, waaronder begrepen informatie vergaard door buitenlandse inlichtingen- en veiligheidsdiensten zonder deugdelijke grondslag in de Nederlandse wet;

II. De Staat te verbieden gegevens van buitenlandse inlichtingen- en veiligheidsdiensten te ontvangen en/of te gebruiken die zijn verkregen in strijd met het Nederlands recht en/of één of meer van de internationale verdragsverplichtingen als bedoeld onder I, en/of van gegevens waarvan niet met zekerheid is vast te stellen dat dit niet het geval is;

III. De Staat ertoe te gelasten om alle passende maatregelen te treffen om de persoonlijke levenssfeer en/of de vrijheid van nieuwsgaring van eisers te beschermen alsmede – wat betreft eisers 6 t/m 9 – van degenen wier belangen zij ingevolge hun statuten behartigen, in het bijzonder door:

   i. betrokkenen betreffende wie de Staat gegevens heeft ontvangen van buitenlandse inlichtingen- en veiligheidsdiensten, zulks in strijd met het Nederlands recht en/of één of meer van de internationale verdragsverplichtingen als bedoeld onder I, althans gegevens waarvan niet met zekerheid is vast te stellen dat dit niet het geval is, binnen drie maanden na betekening van het te dezen te wijzen vonnis daarover zoveel mogelijk schriftelijk te informeren, in ieder geval over de betreffende periode, de aard en de hoeveelheid gegevens, de doeleinden waarvoor de gegevens zijn verzameld

alsmede, desverzocht door de betrokkenen, van de gegevens een kopie aan de betrokkenen te verstrekken;

ii. betrokkenen de mogelijkheid te bieden uitsluitsel te verkrijgen omtrent het al dan niet door de Staat hebben ontvangen van gegevens betreffende hun persoon van buitenlandse inlichtingen- en veiligheidsdiensten, zulks in strijd met het Nederlands recht en/of één of meer van de internationale verdragsverplichtingen als bedoeld onder I, althans gegevens waarvan niet met zekerheid is vast te stellen dat dit niet het geval is, één en ander binnen twee weken na betekening van het te dezen te wijzen vonnis; en/of

iii. gegevens betreffende betrokkenen die de Staat heeft ontvangen van buitenlandse inlichtingen- en veiligheidsdiensten, zulks in strijd met het Nederlands recht en/of één of meer van de internationale verdragsverplichtingen als bedoeld onder I, althans gegevens waarvan niet met zekerheid is vast te stellen dat dit niet het geval is, binnen drie maanden na betekening van het te dezen te wijzen vonnis te wissen.

IV. De Staat in de kosten van deze procedure te veroordelen.

De kosten dezes van mij deurwaarder bedragen:

Deurwaarder

Deze zaak wordt behandeld door
Mr Chr.A. Alberdingk Thijm en Mr C.F.M. de Vries
bureau Brandeis
Keizersgracht 203 1016 DS Amsterdam The Netherlands
T: 020 7606 505 / F: 020 7 606 555
info@bureaubrandeis.com / bureaubrandeis.com