**Rechtbank Den Haag**
Zitting van 5 februari 2014
Nr. C/09/455237, 2013/1325

**Conclusie van antwoord**

inzake

**De Staat der Nederlanden (Ministerie van Binnenlandse Zaken en Koninkrijkrelaties en Ministerie Van Defensie)**
**gedaagde**
advocaat: mr. E.J. Daalder en
mr. drs. C.M. Bitter

tegen

**Bart Theophilus Nooitgedagt, Brenno Johan Simon Aymard August Frans de Winter, Johannes Cornelis van Beek, Robbert Valentijn Gonggrijp, Mathieu Hendrik Paapst, Nederlandse Vereniging voor Strafrecht Advocaten, Nederlandse Vereniging voor Journalisten, Internet Society Nederland, Stichting Privacy First**
wonende te Amsterdam,
**eisers**
advocaat: mr. Chr. A. Alberdingk Thijm

## 1 Inleidende opmerkingen

1.1 Gedaagde – hierna de Staat – ontkent en betwist al hetgeen eisers in de dagvaarding stellen, behoudens voor zover dat in het navolgende uitdrukkelijk wordt erkend.

1.2 De Staat betwist meer in het bijzonder de door eisers als feiten gepresenteerde (veronder)stellingen die betrekking hebben op de vergaring van informatie door de Nederlandse inlichtingendiensten AIVD en MIVD en de uitwisseling van gegevens door deze diensten met buitenlandse diensten. Deze (veronder)stellingen zijn in hoofdzaak gebaseerd op krantenpublicaties. De Staat zal hieronder voor zover mogelijk nader op die (veronder)stellingen reageren.

1.3 De Staat wil uw Rechtbank graag volledig informeren. Tegelijkertijd doet zich hier de bijzonderheid voor dat de nationale veiligheid en de in verband daarmee in artikel 85 Wet op de inlichtingen- en veiligheidsdiensten 2002 (WIV 2002) neergelegde geheimhoudingsplicht zich ertegen verzetten dat bepaalde informatie openbaar wordt. Zoals hierna zal worden toegelicht, voorziet de WIV 2002 om die reden in toezichtsmechanismen om de rechtmatigheid van het handelen van de inlichtingendiensten te borgen.

1.4 De Staat wijst meer in het bijzonder op de Commissie betreffende de inlichtingen- en veiligheidsdiensten (CTIVD) als bedoeld in artikel 64 WIV 2002. De CTIVD is een onafhankelijk toezichtsorgaan, dat voor de uitvoering van haar wettelijke taak beschikt over verregaande bevoegdheden. Zo heeft de CTIVD toegang tot alle relevante informatie bij de inlichtingendiensten en heeft zij de mogelijkheid tot het horen van medewerkers van de diensten en het – eventueel onder ede – horen van getuigen en deskundigen. Over de kwesties die in deze zaak door eisers aan de orde worden gesteld – kort gezegd de verzameling en uitwisseling van gegevens van Nederlanders door buitenlandse inlichtingendiensten, in het bijzonder de Amerikaanse NSA, zal de CTIVD in februari 2014 een rapport vaststellen, dat relevant zal zijn voor beoordeling van de argumenten van eisers. Het rapport is gericht tot de Minister van Binnenlandse Zaken en Koninkrijksrelaties (hierna: de Minister van BZK) en de Minister van Defensie. Na vaststelling van het rapport door de CTIVD moet het rapport, met een reactie van het kabinet daarop, binnen zes weken aan de Tweede Kamer worden toegezonden. De Staat zal dit rapport met de reactie na verschijning in het geding brengen.

1.5 De Staat is voorts bereid om, indien uw Rechtbank dat voor de beoordeling van de vordering nodig zou achten en daarom, bijvoorbeeld met toepassing van artikel 22 Rv, zou verzoeken, geheime informatie vertrouwelijk, door analoge toepassing van artikel 8:29 Awb, aan uw rechtbank ter kennis te brengen. De Staat wijst in dit verband op het arrest van de Hoge Raad van 11 juli 2008, ECLI:NL:HR:2008:BC8421, dat in deze mogelijkheid voorziet en daarvoor een procedure schetst.

## 2 Samenvatting van het standpunt van de Staat

2.1 Eisers leggen aan hun vorderingen het uitgangspunt ten grondslag dat Nederlandse inlichtingendiensten geen gegevens van buitenlandse inlichtingendiensten zouden mogen ontvangen of gebruiken die in strijd met Nederlands recht en/of voor Nederland geldende internationale verdragsverplichtingen door buitenlandse inlichtingendiensten zijn verzameld. Dat uitgangspunt gaat van de onjuiste veronderstelling uit dat buitenlandse inlichtingendiensten bij het verzamelen en verstrekken van gegevens aan Nederlandse inlichtingendiensten aan de Nederlandse wet- en regelgeving zijn gebonden, althans dat het gebruik van die gegevens door Nederlandse inlichtingendiensten alleen dan rechtmatig is als de gegevens zijn verzameld en uitgewisseld in overeenstemming met Nederlandse wet- en regelgeving.

2.2 Dit uitgangspunt is zowel juridisch onjuist als praktisch niet toepasbaar. De Staat zal dit hierna toelichten, maar hecht er aan om eerst uitdrukkelijk vast te leggen dat:

(i) de Staat er niet mee bekend is dat door buitenlandse inlichtingendiensten en meer in het bijzonder de NSA gegevens, waaronder metadata zijn verzameld en met Nederlandse inlichtingendiensten zijn gedeeld, die door buitenlandse inlichtingendiensten zijn verzameld door middel van een inbreuk op de Nederlandse rechtssfeer of soevereiniteit;

(ii) Nederlandse inlichtingendiensten evenmin aan buitenlandse inlichtingendiensten, waaronder de NSA, hebben gevraagd om verzameling of verstrekking van gegevens, waaronder metadata, waarvan bekend is dat die zijn of worden verzameld op een wijze die een ongeoorloofde inbreuk op de persoonlijke levenssfeer oplevert.

2.3 De Staat stelt voorop dat een goede samenwerking met buitenlandse diensten van wezenlijk belang is voor een adequate taakvervulling door de inlichtingendiensten. De gegevens die door deze samenwerking worden verkregen, versterken in belangrijke mate de bestaande informatiepositie van de diensten, die daardoor beter in staat zijn risico's voor de nationale veiligheid in te schatten en de verantwoordelijke autoriteiten hiervoor tijdig te waarschuwen.

> Vgl. Kamerstukken II, 1997/1998, 25 877, nr. 3, p. 73-74 en Kamerstukken II, 1999/2000, 25 877, nr. 8, p. 101.

De WIV 2002 legt daarom op de hoofden van de diensten de verplichting zorg te dragen voor het onderhouden van verbindingen met daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen.

2.4 De steeds verder gaande internationalisering en de snelle technologische ontwikkelingen maken dat een goede samenwerking met buitenlandse diensten een absolute noodzaak is voor inlichtingendiensten om hun wettelijke taken uit te kunnen voeren. Veiligheidsproblemen hebben de laatste jaren in toenemende mate een grensoverschrijdend en internationaal karakter. Teneinde de doelmatigheid en doeltreffendheid van de diensten te vergroten is samenwerking met inlichtingen- en veiligheidsdiensten van andere landen daarom onontbeerlijk. Om met betrekking tot een bepaald onderwerp een zo compleet mogelijk beeld te krijgen kan het bijvoorbeeld wenselijk zijn een vergelijkbare dienst te vragen of zij eventueel informatie over het desbetreffende onderwerp heeft of, indien dat niet het geval is, haar contacten te gebruiken om alsnog aan informatie te komen. Samenwerking vloeit bovendien voort uit in internationale verdragen door de Staat gemaakte afspraken. Zo bestaat een juridisch bindend stelsel van internationale verdragen om proliferatie van kernwapens en kernwapentechnologie, het nemen van kernproeven en de ontwikkeling en het bezit van biologische en chemische wapens tegen te gaan.

Enkele voorbeelden:
Verdrag van de VN inzake het recht van de zee, Trb. 1984, 55 (artikel 100)
Internationaal Verdrag ter bestrijding van daden van nucleair terrorisme, Trb. 2005, 290 (artikel 7)
Verdrag inzake de bestrijding van terroristische bomaanslagen, Trb. 1998, 84 (artikel 15);
Europees Verdrag ter voorkoming van terrorisme, Trb. 2006, 34 (artikel 3, lid 2 sub a, artikel 4 en artikel 22)

2.5 De samenwerking met inlichtingen- en veiligheidsdiensten van andere landen is niet eenzijdig. Naast de hiervoor genoemde internationale verdragsverplichtingen achten buitenlandse inlichtingen- en veiligheidsdiensten het met het oog op hun eigen activiteiten van belang bepaalde informatie van de Nederlandse diensten te krijgen. De wetgever heeft voor ogen gehad dat verzoeken om dergelijke informatie te verschaffen in beginsel positief tegemoet moeten worden getreden, teneinde er in voldoende mate van verzekerd te blijven dat dit andersom ook gebeurt bij verzoeken om informatie van de Nederlandse diensten aan deze diensten.

Kamerstukken II, 1997/1998, 25 877, nr. 3, p. 73/74.

2.6 Door deze samenwerking / door het inwilligen van verzoeken van de buitenlandse dienst in kwestie wordt daardoor, indirect, de eigen nationale veiligheid gediend. Dat geldt dus over en weer: het wederkerigheidsbeginsel (quid pro quo) vormt de basis voor een goede internationale samenwerking en zonder wederkerigheid is een goede internationale samenwerking niet mogelijk. Inlichtingen- en veiligheidsdiensten zullen elkaar, voor zover en waar dat mogelijk is, bijstaan.

2.7 Het voorgaande betekent ook dat ingeval van toewijzing van de vorderingen belangrijke principes van samenwerking zouden moeten worden verlaten en internationale verplichtingen niet meer zouden kunnen worden nageleefd. Dat betekent ook dat buitenlandse diensten ingeval van toewijzing de samenwerking zullen heroverwegen en dat ervan uit moet worden gegaan dat zij de samenwerking zullen beëindigen, althans dat de meest belangrijke samenwerkingsrelaties zullen worden beëindigd. Daar komt bij dat toewijzing van de vorderingen zou betekenen dat AIVD en MIVD zouden moeten vragen naar bronnen en methodes van buitenlandse inlichtingendiensten waarmee zij samenwerken. Omgekeerd zouden AIVD en MIVD dergelijke informatie niet aan buitenlandse inlichtingendiensten mogen verstrekken; artikel 15 WIV 2002 staat daaraan in de weg. Het zou bovendien betekenen dat buitenlandse diensten hun systeem zouden moeten aanpassen, omdat zij de informatie waarom de Staat volgens de eisers zou moeten vragen niet in die vorm in hun systemen registreren. Het hoeft geen betoog dat zij dat niet zullen doen. Van internationale samenwerking zal dan de facto geen sprake meer zijn. Dat doet ernstig afbreuk aan de adequate bescherming van de nationale veiligheid, daaronder begrepen een ongestoorde voorbereiding en inzet van de krijgsmacht.

2.8 Buitenlandse inlichtingendiensten zijn niet gehouden hun bronnen en werkwijzen aan Nederlandse inlichtingendiensten prijs te geven en zullen dat ook niet doen. Dat is staande praktijk bij de uitwisseling van gegevens tussen inlichtingendiensten. AIVD en MIVD mogen dergelijke informatie als gezegd op grond van artikel 15 WIV 2002 ook niet aan buitenlandse inlichtingendiensten verstrekken.

2.9 Dat buitenlandse inlichtingendiensten geen informatie geven over hun bronnen of de wijze waarop zij uitgewisselde informatie hebben vergaard staat niet aan het gebruik van gegevens door Nederlandse inlichtingendiensten in de weg. Nederlandse inlichtingendiensten mogen bij de toepassing van de WIV 2002 gebruik maken van alle door een buitenlandse inlichtingendienst verstrekte informatie, ongeacht de wijze waarop de buitenlandse inlichtingendienst de informatie heeft verkregen. Dat geldt in ieder geval voor de informatie waar het in deze zaak om gaat, de uitwisseling van metadata.

2.10 Uitwisseling van metadata met buitenlandse diensten vindt uitsluitend plaats binnen samenwerkingsrelaties. Een goede samenwerkingsrelatie met buitenlandse inlichtingendiensten is onontbeerlijk voor een behoorlijke taakvervulling van inlichtingendiensten. Daardoor wordt de informatiepositie van die diensten versterkt, waardoor risico's voor de nationale veiligheid beter kunnen worden ingeschat en de noodzakelijke maatregelen kunnen worden getroffen.

2.11 Uitgangspunt is dat op basis van de criteria die bij de selectie van samenwerkingspartners en het vorm geven van die relatie worden gehanteerd (zoals respect voor mensenrechten, democratische inbedding, professionaliteit en

betrouwbaarheid), sprake is van een dienst waarmee op grond van artikel 59 WIV 2002 voor dit doel mag worden samengewerkt. De samenwerking van de AIVD met buitenlandse diensten is onderwerp geweest van het rapport nr. 22A van de CTIVD (productie 17). In dat rapport wordt onder meer nader ingegaan op de wijze waarop aan de criteria invulling wordt gegeven:

> "(...)
> Artikel 59 lid 1 WIV 2002 legt aan het hoofd van de AIVD de zorgplicht op om verbindingen te onderhouden met daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen. Een goede samenwerkingsrelatie met buitenlandse diensten is van wezenlijk belang voor een adequate taakvervulling door de AIVD. De gegevens die door deze samenwerking worden verkregen, versterken namelijk in belangrijke mate de bestaande informatiepositie van de AIVD die daardoor beter in staat is risico's voor de nationale veiligheid in te schatten en de verantwoordelijke autoriteiten hiervoor tijdig te waarschuwen. Met name sinds de aanslagen van 11 september 2001 is de noodzaak van internationale samenwerking tussen inlichtingen- en veiligheidsdiensten duidelijker geworden en de bereidwilligheid daartoe toegenomen.
>
> De samenwerkingsrelaties tussen de AIVD en buitenlandse diensten verschillen van collega-dienst tot collega-dienst en zijn veelal aan verandering onderhevig. Samenwerking bestaat doorgaans grotendeels uit de uitwisseling van gegevens. Daarnaast worden er met bepaalde collega-diensten gezamenlijke operaties uitgevoerd en worden technische en andere vormen van ondersteuning verleend. Tevens vinden er expertmeetings plaats van bijvoorbeeld juristen, technici en andere deskundigen. Ook wordt er samengewerkt op het gebied van personeelsopleidingen en -trainingen. De intensiteit en de frequentie van de samenwerking binnen de diverse bilaterale relaties van de AIVD lopen sterk uiteen. Zo kan er onderscheid gemaakt worden in samenwerkingsrelaties met een meer protocollair, *ad hoc*, tactisch of operationeel karakter. Voorts kan er op een specifiek taakveld intensief worden samengewerkt terwijl op andere onderwerpen terughoudendheid wordt betracht. (p. 7)
> (...)
> De democratische inbedding en het respect voor de mensenrechten van een buitenlandse dienst dienen een essentieel onderdeel uit te maken van de besluitvorming omtrent het aangaan en onderhouden van relaties met de desbetreffende dienst. Dit ligt in het verlengde van artikel 59 WIV 2002 waarin, onder meer, is bepaald dat de samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten slechts plaatsvindt voorzover de belangen die zij behartigen niet onverenigbaar zijn met de belangen die de AIVD heeft te behartigen, waaronder 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.

Of een dienst in voldoende mate democratisch is ingebed, hangt af van een aantal factoren. Zo kan onder meer worden gekeken naar het algehele politieke bestel van het land in kwestie en de positie die de desbetreffende dienst daarin inneemt, de wettelijke bevoegdheden van de dienst en het (onafhankelijke) toezicht daarop. Met betrekking tot het criterium respect voor de mensenrechten, kan onder meer bezien worden of het desbetreffende land internationale mensenrechtenverdragen heeft geratificeerd en of deze mensenrechtenverdragen in de praktijk nageleefd worden. Eveneens is het van belang of een buitenlandse collega-dienst in verband wordt of is gebracht met schendingen van mensenrechten. Zo kan, bijvoorbeeld, worden gekeken naar signaleringen van schendingen van mensenrechten in onderzoeken en rapporten van nationale en internationale mensenrechtenorganisaties. (p. 8).
(...)
De mate waarin een buitenlandse collega-dienst als professioneel en als betrouwbaar kan worden beschouwd is grotendeels afhankelijk van de ervaringen van de AIVD die zijn opgedaan in de samenwerkingsrelatie met de betrokken dienst. Dit criterium is bijgevolg minder bruikbaar en de invulling daarvan moeilijker te beoordelen ten tijde van het aangaan van een samenwerkingsrelatie. Wel worden met andere (bevriende) collega-diensten opvattingen en ervaringen in dit kader uitgewisseld, wat kan bijdragen aan de inschatting of een buitenlandse dienst professioneel en betrouwbaar is. De professionaliteit en betrouwbaarheid van een collega-dienst zijn voorts belangrijke factoren bij de besluitvorming omtrent een eventuele intensivering van de samenwerkingsrelatie. Wanneer er aanwijzingen zijn dat een collega-dienst onprofessioneel te werk gaat dan wel onbetrouwbaar is, dan kan en mag de AIVD er niet op vertrouwen dat deze collega-dienst zich aan de gemaakte afspraken zal houden. De samenwerking zal dan slechts oppervlakkige vormen kunnen aannemen. (p. 10/11)

2.12 Wordt een samenwerkingsrelatie aangegaan dan betekent dit dat er voor zover die samenwerking strekt voldoende vertrouwen in de professionaliteit en betrouwbaarheid van de betreffende dienst bestaat en ook mag bestaan. Hoe sterker dat vertrouwen is, hoe intensiever de samenwerkingsrelatie kan gaan. De samenwerkingsrelatie kan dus verschillen naarmate aan de buitenlandse dienst aan de hiervoor weergegeven criteria voldoet. De uitersten zijn enerzijds een protocollaire samenwerking en anderzijds gezamenlijke onderzoeken en joint operations.

2.13 Nederlandse inlichtingendiensten zullen bij de buitenlandse dienst geen navraag doen naar de bronnen en/of gebruikte methoden en technieken en doen dat ook niet. De buitenlandse dienst zal deze bronnen of methoden en technieken niet verstrekken.

Omgekeerd vraagt de buitenlandse dienst daar ook niet om en zouden de Nederlandse inlichtingendiensten die informatie ook niet verstrekken. Soms kunnen in bepaalde samenwerkingsrelaties bronnen bekend zijn (bijvoorbeeld als gebruik wordt gemaakt van dezelfde menselijke bron) of kan bekend zijn welke methode er is gebruikt (bijvoorbeeld interceptie), maar dan niet op welke wijze die methode is gebruikt. Buiten die gevallen kan dat niet. Dat betekent dus dat inherent aan de samenwerkingsrelaties, Nederlandse inlichtingendiensten niet in de positie of in staat zijn om de gebruikte bronnen of methoden en technieken te controleren en dat zij zich dus ook, anders dan eisers voorstaan, geen oordeel kunnen vormen over de vraag of de gegevens in strijd met Nederlandse wet- en regelgeving zijn verkregen.

2.14 Dat is ook niet noodzakelijk omdat voor de vraag of een buitenlandse inlichtingendienst de informatie op rechtmatige wijze heeft verkregen, niet de Nederlandse wet- en regelgeving of maatstaven gelden, maar de regelgeving dat het handelen van de betrokken buitenlandse dienst beheerst. Voor door de NSA aan Nederlandse inlichtingendiensten verstrekte gegevens betekent dit dat de rechtmatigheid van de verzameling van gegevens wordt beheerst door de hierna beschreven (onder 3.3) Amerikaanse regelgeving, meer in het bijzonder de FISA, en is onderworpen aan de toezichts- en controlemiddelen in de Verenigde Staten. In het kader van de uitwisseling van gegevens is vervolgens het vertrouwen in het opereren van de buitenlandse dienst dat de grondslag heeft gevormd voor het aangaan en voortzetten van de hechte samenwerkingsrelatie voldoende om vast te stellen dat de uitwisseling van informatie op grond van artikel 59 WIV 2002 rechtmatig is.

2.15 Dat betekent dat ook informatie die de buitenlandse dienst heeft verzameld op een wijze die niet in de WIV 2002 is vastgelegd door die dienst aan Nederlandse inlichtingendiensten rechtmatig mag worden verstrekt en vervolgens door de Nederlandse diensten worden gebruikt. Het feit dat Nederlandse regelgeving niet voorziet in een bepaalde vorm van informatieverzameling waarin de voor de buitenlandse dienst toepasselijke regelgeving wel voorziet, betekent niet dat de verzameling en verstrekking van die informatie aan en het vervolgens door de diensten gebruiken van die informatie een onaanvaardbare inbreuk op de persoonlijke levenssfeer zou opleveren.

2.16 Dat geldt ook voor de zg. *kabelgebonden interceptie,* die in de dagvaarding wordt genoemd en die door de NSA, zoals uit de hierna genoemde uitspraken van de beide District Judges blijkt (randnummers 3.3.12 en 3.3.13), ook wordt toegepast. De WIV 2002 kent techniekafhankelijke bevoegdheden, interceptie van niet-kabelgebonden telecommunicatie die zijn oorsprong of bestemming in andere landen heeft ter verkenning van de communicatie (artikel 27 WIV 2002) en ongerichte interceptie van niet-kabelgebonden telecommunicatie (artikel 27 WIV 2002). De WIV 2002 staat gerichte interceptie van kabelgebonden telecommunicatie toe (artikel 25 WIV 2002), maar voorziet niet in een grondslag voor *ongerichte* interceptie van kabelgebonden

telecommunicatie. De Evaluatiecommissie WIV 2002 (de commissie Dessens) heeft de regering overigens geadviseerd om het wettelijk mogelijk te maken dat Nederlandse inlichtingendiensten de bevoegdheid krijgen om ongericht kabelgebonden telecommunicatie te intercepteren. De Regering zal hierover in maart 2014 een standpunt innemen.

> *Kamerstukken II,* 2013/2014, 33820, nr. 1
> Rapport Commissie Dessens (http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/12/02/rapport-evaluatie-wiv-2002.html), p. 76/7.

2.17 Het feit dat de Nederlandse wetgeving inlichtingendiensten niet toestaat om ongericht kabelgebonden telecommunicatie te intercepteren, verzet zich er niet tegen dat de diensten gebruik maken van gegevens die door een buitenlandse inlichtingendienst met deze methode zijn verkregen. Meer in het bijzonder geldt dat voor gegevens van de NSA, omdat voor deze methode een uitdrukkelijk basis in Amerikaanse regelgeving bestaat. Het op deze wijze door de NSA verzamelen en uitwisselen van metadata met Nederlandse inlichtingendiensten is dus rechtmatig. Datzelfde geldt voor het gebruik van die informatie. Artikel 59 WIV 2002 voorziet daarin. Dit artikel bevat niet de beperking dat die uitwisseling alleen toelaatbaar is als aan de criteria van de WIV 2002 is voldaan. Vanzelfsprekend gelden de artikelen 12 e.v., de algemene regels voor de verwerking van persoonsgegevens, wel.

## 3 Feiten en achtergronden

### *3.1 De gebeurtenissen sinds juni 2013*

3.1.1 Op 6 juni 2013 werd bekend dat Edward Snowden, een voormalige contractant van de Amerikaanse *National Security Agency* (hierna: NSA), ongeveer 200.000 geclassificeerde documenten van de NSA beschikbaar heeft gesteld aan de pers. Deze documenten hebben hoofdzakelijk betrekking op de activiteiten van de NSA en in beperktere mate op activiteiten van inlichtingendiensten van andere landen, zoals de Britse inlichtingendienst *Government Communications Headquarters* (hierna: GCHQ).

3.1.2 Met name de Britse krant *The Guardian* en de Amerikaanse krant *The Washington Post* hebben sindsdien informatie uit de gelekte documenten gepubliceerd. Deze eerste publicaties betroffen met name het door de NSA gebruikte programma 'PRISM', een computersysteem voor de vergaring van buitenlandse informatie van aanbieders van elektronische communicatie voor inlichtingendoeleinden.

3.1.3 De Minister van BZK heeft bij brief van 21 juni 2013 namens het kabinet een reactie op de berichten in de media over het Amerikaanse programma PRISM aan de Tweede Kamer toegezonden. De Minister van BZK heeft in deze brief het kader uiteengezet waarbinnen de Nederlandse inlichtingen- en veiligheidsdiensten opereren, waaronder

het kader voor samenwerking met buitenlandse inlichtingendiensten. De Minister van BZK heeft voorts aangegeven dat de AIVD en de MIVD het computerprogramma PRISM niet gebruiken. Als bijlage bij deze brief is een 'Factsheet' van de Amerikaanse Director of National Intelligence' van 8 juni 2013 aan de Tweede Kamer toegestuurd.

> Zie: *Kamerstukken II* 2012/2013, 30 977, nr. 56, met als bijlage 'Director of National Intelligence, Washington, DC 20511, June 8, 2013 'Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" (**productie 1**).

3.1.4 Uit deze factsheet volgt dat PRISM een intern computersysteem is van de Amerikaanse overheid dat wordt gebruikt om de vergaring van buitenlandse inlichtingen te faciliteren. De vergaring van deze informatie is gebaseerd op Section 702 van de *Foreign Intelligence Surveillance Act* (hierna: FISA).

> Zie voorts: Council of the European Union, Report on the findings by the EU Co-chairs and the ad hoc EU-US Working Group on Data Protection, 27 November 2013, 16987/13, p. 4 (**productie 2**).

3.1.5 Bij brief van 3 juli 2013 heeft de Minister van BZK de Tweede Kamer nader geïnformeerd over de samenwerking van de AIVD en de MIVD met de NSA:

> "De mate van samenwerking met een buitenlandse dienst wordt onder meer bepaald op basis van de democratische inbedding van de collega-dienst, het respect voor de mensenrechten van het desbetreffende land, de betrouwbaarheid en de professionaliteit van de dienst en het operationele belang van de samenwerking. (...) Over de vorm van samenwerking met specifieke buitenlandse diensten worden in het openbaar geen mededelingen gedaan. Internationale samenwerking is noodzakelijk voor de taakuitvoering van de diensten en vindt plaats binnen het kader van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002).
>
> (...)
>
> De AIVD en MIVD zijn niet bevoegd verzoeken te doen aan buitenlandse collega-diensten en activiteiten uit te voeren die de WIV 2002 de Nederlandse diensten niet toestaat. Dat geldt ook voor ongerichte interceptie van de kabelinfrastructuur.
>
> Het is 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. Voor zover in het kader van de internationale samenwerking collega-diensten hun werkwijzen bij de AIVD of de MIVD bekend hebben gemaakt, worden hierover in het openbaar geen mededelingen gedaan."
>
> Zie: *Kamerstukken II* 2012/2013, 30 977, nr. 59 (**productie 3**).

3.1.6 Bij brief van 16 juli 2013 heeft de Tweede Kamer de CTIVD verzocht onderzoek te verrichten naar de dataverzameling door de AIVD en de MIVD. De Tweede Kamer heeft onder meer verzocht de omvang en aard van de datavergaring, de relatie tussen vergaring en uitwisseling van gegevens met buitenlandse diensten en de verhouding van datavergaring en uitwisseling tot het recht op bescherming van de persoonlijke levenssfeer te onderzoeken.

Zie: Brief Voorzitter van de Tweede Kamer van 16 juli 2013 (**productie 4**).

3.1.7 Bij brief van 5 augustus 2013 aan de Voorzitter van de Tweede Kamer heeft de CTIVD aangekondigd een onderzoek te zullen verrichten naar bepaalde aspecten van gegevensverwerking op het gebied van telecommunicatie door de AIVD en MIVD. In dat onderzoek zal in ieder geval aandacht worden besteed aan de volgende onderwerpen:

1. De reikwijdte van de algemene en bijzondere bevoegdheden van de diensten tot gegevensverwerking op het gebied van telecommunicatie, mede in relatie tot de Grondwet en het EVRM.
2. De wijze waarop gebruik wordt gemaakt van verschillende soorten gegevensbestanden door de diensten en de regels die gelden voor dat gebruik.
3. De mogelijkheden en beperkingen van de uitwisseling van gegevens met buitenlandse inlichtingen- en/of veiligheidsdiensten.
4. De wijze waarop de door het EVRM gestelde toetsingsnormen – noodzakelijkheid, proportionaliteit en subsidiariteit – een rol spelen bij de gegevensverwerking door de diensten, in het bijzonder bij de gegevensuitwisseling met buitenlandse inlichtingen- en/of veiligheidsdiensten.

Zie: Brief CTIVD van 5 augustus 2013 (**productie 5**).

De Minister van BZK heeft tijdens het algemeen overleg op 6 november 2013 aan de Vaste commissie voor Binnenlandse Zaken van de Tweede Kamer toegezegd een door het kamerlid Schouw geconstateerd verschil tussen het verzoek van de Tweede Kamer aan de CTIVD en het door de CTIVD aangekondigde onderzoek onder de aandacht van de CTIVD te brengen. Dat is bij brief van 12 november 2013 gebeurd. De CTIVD heeft hierop aangegeven dat zij in haar onderzoek onder gegevensverwerking op grond van artikel 1 WIV 2002 ook gegevensverzameling verstaat, en voorts dat zij niet alleen onderzoek doet naar de mogelijkheden, maar ook naar de feiten op het gebied van de samenwerking tussen de AIVD en de MIVD met buitenlandse diensten.

Zie: *Kamerstukken II* 2013/2014, 30 977, nr. 76 (**productie 6**).

3.1.8 Op de website Tweakers.net werd op 21 oktober een bericht geplaatst, gebaseerd op een krantenartikel in de Franse krant 'Le Monde' van diezelfde datum, dat de NSA in

2012 in een maand tijd ongeveer 1,8 miljoen telefoongesprekken in Nederland zou hebben onderschept.

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

3.1.9 Bij brief van 28 oktober 2013 heeft de Minister de Tweede Kamer geïnformeerd over de berichtgeving op Tweakers.net. De Minister heeft aangegeven dat het kabinet gelet op de bepalingen van de Amerikaanse FISA, zich ervan bewust is dat de NSA telefooncommunicatie kan onderscheppen. De berichtgeving op Tweakers.net heeft betrekking op het onderscheppen van metadata. De Minister acht het intercepteren van metadata en het analyseren daarvan in zijn algemeenheid een aanvaardbare methode in het kader van onderzoek naar terroristen, andere gevaren voor de nationale veiligheid of in het kader van militaire operaties. In Nederland vormen artikel 26 en 27 jo. artikelen 12 e.v. van de WIV 2002 daarvoor de wettelijke basis. Over het verzamelen van inlichtingen door buitenlandse inlichtingendiensten in of vanuit Nederland, gaf de Minister het volgende aan:

> "Het kan voorkomen dat andere landen menen dat er een goede reden is om in of vanuit Nederland inlichtingen te verzamelen. In een dergelijk geval dient het desbetreffende land een verzoek te richten tot de AIVD of de MIVD. Het verzoek wordt dan binnen de kaders van de Nederlandse wet beoordeeld. Het kabinet acht enig optreden buiten die wettelijke kaders niet aanvaardbaar. De AIVD en de MIVD doen om die reden structureel onderzoek naar spionage van buitenlandse mogendheden in Nederland. Indien dergelijke spionage wordt geconstateerd, dan volgen altijd maatregelen. Dat geldt ook als bondgenoten ongewenste spionageactiviteiten in Nederland uitvoeren, In Nederland geldt de Nederlandse wet, ook voor bondgenoten."
>
> Zie: *Kamerstukken II* 2013/2014, 30 977, nr. 63, p. 1-2 (**productie 7**).

3.1.10 De NSA heeft in reactie op de berichtgeving over de vergaring van gespreksgegevens aangegeven dat het niet gaat om de inhoud van gesprekken, maar om aantekeningen van metadata. Die metadata zijn verzameld door de rechtmatige toepassing van bevoegdheden van de NSA of verkregen van buitenlandse samenwerkingspartners van de NSA.

> "statement on articles in European press alleging large numbers of phone call metadata collected by NSA in France, Spain, Italy
>
> The assertions by reporters in France (Le Monde), Spain (El Mundo) and Italy (L'Espresso) that NSA collected 10s of millions of phone calls are completely false. They cite as evidence screen shots of the results of a web tool used for data management purposes, but both they and the person who stole the classified data did not understand what they were looking at. The web tool counts metadata records from around the world and displays the totals in

several different formats. The sources of metadata include data legally collected by NSA under its various authorities, as well as metadata provided to NSA by foreign partners. To be perfectly clear, this is not information that we collected on European citizens. It represents information that we and our NATO allies have collected in defense of our countries and in support of military operation."

Zie: *Kamerstukken II* 2013/2014, 30 977, nr. 64, p. 1 (**productie 8**).

Zie voorts: *Kamerstukken II* 2013/2014, 30 977, nr. 75, p. 23-25 (**productie 9**).

3.1.11 Bij brief van 5 november 2013 heeft de Minister van BZK gereageerd op een bericht in de Volkskrant op 4 november 2013 dat de Nederlandse inlichtingen- en veiligheidsdiensten met buitenlandse inlichtingen- en veiligheidsdiensten zouden samenwerken in een samenwerkingsverband genoemd de 'nine eyes'. De Minister gaf aan dat door de AIVD en MIVD wordt samengewerkt met andere inlichtingen- en veiligheidsdiensten en dat deze samenwerking plaatsvindt binnen de kaders van de WIV 2002. Over de samenwerking met de Verenigde Staten heeft de Minister van BZK tijdens het algemeen overleg met de vaste commissie voor Binnenlandse Zaken aangegeven dat als bondgenoten wordt samengewerkt.

Zie:
- *Kamerstukken II* 2013/2014, 30 977, nr. 65 (**productie 10**);
- *Kamerstukken II* 2013/2014, 30 977, nr. 75, p. 18 (**productie 11**).

3.1.12 Vanaf 23 november 2013 publiceert NRC Handelsblad een serie artikelen op basis van de gelekte documenten van de NSA. De Minister heeft naar aanleiding van berichtgeving in NRC Handelsblad van 23 november 2013 dat Nederland in het verleden doelwit zou zijn geweest van de Amerikaanse NSA aangegeven dat de NSA eerder heeft gemeld dat Nederland thans geen doelwit is. Indien buitenlandse inlichtingen- en veiligheidsdiensten in of vanuit Nederland inlichtingen willen verzamelen met het oog op hun taakuitoefening, dient daarvoor een verzoek te worden gericht aan de AIVD of de MIVD. Dit verzoek wordt door de AIVD of de MIVD beoordeeld op grond van de WIV 2002.

Zie: *Kamerstukken II* 2013/2014, 30 977, nr. 74 (**productie 12**).

3.1.13 De Staat is niet bekend met informatievergaring door de NSA binnen de Nederlandse rechtssfeer buiten het medeweten en de betrokkenheid van de Nederlandse diensten.

Zie ook: *Kamerstukken II* 2013/2014, 30 977, nr. 75, p. 22 (**productie 13**).

## *3.2 De Nederlandse Inlichtingen- en veiligheidsdiensten*

*Taken en bevoegdheden*

3.2.1 De AIVD en MIVD verrichten hun werkzaamheden op grond van de WIV 2002. De activiteiten van beide diensten zijn gericht op de bescherming van de nationale veiligheid. Daartoe heeft de AIVD vijf taken die als volgt zijn omschreven in artikel 6 lid 2 sub a t/m e WIV 2002:

> "a. het verrichten van onderzoek met betrekking tot organisaties en personen die door de doelen die zij nastreven, dan wel door hun activiteiten aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat;
> b. het verrichten van veiligheidsonderzoeken als bedoeld in de Wet veiligheidsonderzoeken;
> c. het bevorderen van maatregelen ter bescherming van de onder a genoemde belangen, waaronder begrepen maatregelen ter beveiliging van gegevens waarvan de geheimhouding door de nationale veiligheid wordt geboden en van die onderdelen van de overheidsdienst en van het bedrijfsleven die naar het oordeel van Onze ter zake verantwoordelijke Ministers van vitaal belang zijn voor de instandhouding van het maatschappelijk leven;
> d. het verrichten van onderzoek betreffende andere landen ten aanzien van onderwerpen die door Onze Minister-President, Minister van Algemene Zaken, in overeenstemming met Onze betrokken Ministers zijn aangewezen;
> e. het opstellen van dreigings- en risicoanalyses op verzoek van Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties en Onze Minister van Veiligheid en Justitie gezamenlijk ten behoeve van de beveiliging van de personen, bedoeld in de artikelen 4, derde lid, onderdeel b, en 42, eerste lid, onder c, van de Politiewet 2012 en de bewaking en de beveiliging van de objecten en de diensten die zijn aangewezen op grond van artikel 16 van die wet."

De taken van de MIVD zijn neergelegd in artikel 7 lid 2 sub a t/m f WIV 2002:

> "a. het verrichten van onderzoek:
> 1°. omtrent het potentieel en de strijdkrachten van andere mogendheden, ten behoeve van een juiste opbouw en een doeltreffend gebruik van de krijgsmacht;
> 2°. naar factoren die van invloed zijn of kunnen zijn op de handhaving en bevordering van de internationale rechtsorde voor zover de krijgsmacht daarbij is betrokken of naar verwachting betrokken kan worden;

b. het verrichten van veiligheidsonderzoeken als bedoeld in de Wet veiligheidsonderzoeken;
c. het verrichten van onderzoek dat nodig is voor het treffen van maatregelen:
1°. ter voorkoming van activiteiten die ten doel hebben de veiligheid of paraatheid van de krijgsmacht te schaden;
2°. ter bevordering van een juist verloop van mobilisatie en concentratie der strijdkrachten;
3°. ten behoeve van een ongestoorde voorbereiding en inzet van de krijgsmacht als bedoeld in onderdeel a, onder 2°.
d. het bevorderen van maatregelen ter bescherming van de onder c genoemde belangen, waaronder begrepen maatregelen ter beveiliging van gegevens betreffende de krijgsmacht waarvan de geheimhouding is geboden;
e. het verrichten van onderzoek betreffende andere landen, ten aanzien van onderwerpen met een militaire relevantie die door Onze Minister-President, Minister van Algemene Zaken, in overeenstemming met Onze betrokken Ministers, zijn aangewezen;
f. het opstellen van dreigingsanalyses op verzoek van Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties en Onze Minister van Veiligheid en Justitie gezamenlijk ten behoeve van de beveiliging van de personen, bedoeld in de artikelen 4, derde lid, onderdeel b, en 42, eerste lid, onder c, van de Politiewet 2012 en de bewaking en de beveiliging van de objecten en de diensten die zijn aangewezen op grond van artikel 16 van die wet, voor zover het betreft personen, objecten en diensten met een militaire relevantie."

3.2.2 Voor de uitoefening van die taken komt aan de AIVD en de MIVD op grond van de WIV 2002 de algemene bevoegdheid toe tot het verzamelen van gegevens (artikel 17 WIV 2002). Daaronder valt ook het verzamelen van persoonsgegevens.

3.2.3 Voorts beschikken de AIVD en de MIVD over bijzondere bevoegdheden die kunnen worden toegepast voor zover noodzakelijk voor de goede uitvoering van de 'a-taak' en 'd-taak' van de AIVD en voor de 'a-taak', 'c-taak' en 'e-taak' van de MIVD. De bijzondere bevoegdheden zijn neergelegd in de artikelen 20 t/m 30 WIV 2002. Het gaat daarbij om de bevoegdheid tot observeren en volgen (artikel 20 WIV 2002), het gebruik van agenten (artikel 21 WIV 2002), het doorzoeken van besloten plaatsen, gesloten voorwerpen en het verrichten van onderzoek aan voorwerpen met als doel de vaststelling van de identiteit van een persoon (artikel 22 WIV 2002), het openen van brieven (artikel 23 WIV 2002), het binnendringen in een geautomatiseerd werk (artikel 24 WIV 2002), het gericht afluisteren van communicatie (artikel 25 WIV 2002), het ontvangen en opnemen van niet-kabelgebonden telecommunicatie ter verkenning van de communicatie (artikel 26 WIV 2002), het ongericht ontvangen en opnemen van niet-kabelgebonden telecommunicatie en de selectie daarvan (artikel 26 en artikel 27 WIV 2002), het verkrijgen van verkeers- en abonneegegevens van

telecommunicatiediensten (artikel 28 en 29 WIV 2002) en het betreden van plaatsen (artikel 30 WIV 2002).

3.2.4 Voor de uitoefening van bijzondere bevoegdheden is, voor zover de wet niet anders bepaalt, toestemming van de betrokken Minister of namens deze het hoofd van de dienst vereist. Toestemming van de Minister is in ieder geval vereist bij de bevoegdheid tot gericht afluisteren (artikel 25 WIV 2002) en de selectie van ongericht geïntercepteerde niet-kabelgebonden telecommunicatie (artikel 27, derde lid WIV 2002). Voor de bevoegdheid tot het openen van brieven is een last van de rechtbank Den Haag vereist (artikel 23 WIV 2002). Voorts zijn op de uitoefening van de bijzondere bevoegdheden de beginselen van subsidiariteit en proportionaliteit van toepassing, zoals uitgewerkt in de artikelen 31 en 32 WIV 2002.

3.2.5 Op grond van voornoemde bevoegdheden zijn de AIVD en de MIVD ook bevoegd tot het intercepteren van niet-kabelgebonden telecommunicatie, waaronder metadata. Gerichte interceptie (het "aftappen" van communicatie) vindt plaats op grond van artikel 25 WIV 2002. Op grond van artikel 26 vindt verkenning communicatie in de ether plaats die zijn oorsprong of bestemming heeft in andere landen. De ongerichte interceptie van telecommunicatie, waaronder metadata, vindt plaats op grond van artikel 27 WIV 2002.

> Zie over deze bevoegdheden: Toezichtsrapporten CTIVD nrs. 28 (MIVD) en 31 en 35 (AIVD) (**producties 14, 15 en 16**).

*Samenwerking met buitenlandse diensten*

3.2.6 De samenwerking tussen de AIVD en de MIVD met inlichtingen- en veiligheidsdiensten van andere landen is geregeld in artikel 59 WIV 2002. Op grond van artikel 59 lid 1 WIV 2002 draagt het hoofd van de dienst zorg voor het onderhouden van verbindingen met daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen. Daarbij kunnen gegevens worden verstrekt of technische ondersteuning en andere vormen van ondersteuning worden verleend. Samenwerking vindt alleen plaats als de door de buitenlandse dienst te behartigen belangen niet onverenigbaar zijn met de belangen die door de Nederlandse diensten worden behartigd en als een goede taakuitvoering door de Nederlandse dienst zich niet tegen samenwerking verzet.

3.2.7 Voor de beoordeling of sprake is van (on)verenigbare belangen is onder meer het Nederlandse buitenlandse beleid van belang, waaronder het beleid op het gebied van en respect voor mensenrechten. Voorts zijn de democratische inbedding, de taken, de professionaliteit en de betrouwbaarheid van en goede ervaringen met de buitenlandse dienst van belang. Voornoemde punten worden betrokken in de afweging met een bepaalde buitenlandse dienst intensiever en op meer structurele basis samen te werken.

Zie:
- *Kamerstukken II* 1997/1998, 25 877, nr. 3, p. 74;
- *Aanhangsel Handelingen II* 2004/2005, nr. 749.
- Toezichtsrapport CTIVD nr. 22A, p. 7-8 (**productie 17**)

3.2.8 Indien de AIVD of MIVD op grond van artikel 59 WIV 2002 gegevens verstrekt aan een buitenlandse dienst, is het onderhouden van een goede samenwerkingsrelatie daarbij het uitgangspunt. Die goede samenwerkingsrelatie met buitenlandse diensten is van wezenlijk belang voor de adequate taakuitoefening door de Nederlandse inlichtingen- en veiligheidsdiensten. De AIVD en MIVD werken samen met buitenlandse inlichtingendiensten in multilateraal en bilateraal verband. De samenwerking kan een protocollair, ad hoc, tactisch of operationeel karakter hebben.

3.2.9 In het kader van de samenwerking met buitenlandse diensten kunnen inlichtingen en dus ook metadata tussen de samenwerkende diensten worden uitgewisseld. Het delen van metadata door Nederlandse inlichtingendiensten met buitenlandse inlichtingendiensten vindt plaats indien een verzameling metadata van belang is voor de taakuitoefening van een buitenlandse dienst. Omgekeerd delen buitenlandse inlichtingendiensten metadata met Nederlandse diensten indien dat voor de taakuitoefening van Nederlandse diensten van belang is.

3.2.10 De uitwisseling van data gebeurt op grond van het uitgangspunt *quid pro quo*. Op basis van wederkerigheid ontvangt de AIVD of de MIVD informatie van de buitenlandse dienst die van belang is voor de taakuitoefening van de Nederlandse dienst en vice versa. Dit is een stelregel in de wereld van inlichtingendiensten en vaste praktijk.

3.2.11 De AIVD en de MIVD zijn op grond van artikel 36 lid 1 sub d WIV 2002 bevoegd in het kader van een goede taakuitoefening gegevens te verstrekken aan daarvoor in aanmerking komende buitenlandse diensten. Gegevensverstrekking op basis van deze bepaling vindt plaats op initiatief van de AIVD of MIVD indien de AIVD of MIVD een direct belang heeft bij de verstrekking van de gegevens aan de buitenlandse dienst. De ontvangende dienst mag de verstrekte informatie slechts verder verstrekken indien de Nederlandse dienst daarvoor toestemming heeft gegeven (artikel 37 WIV 2002); deze verplichting geldt overigens ook als het gaat om verstrekking op grond van artikel 59 WIV 2002).

3.2.12 De AIVD en de MIVD verzamelen data op grond van de daarvoor toegekende bevoegdheden in de WIV 2002. Voor zover het gaat om Sigint gebeurt dat met name op grond van artikel 27 WIV 2002. Indien de AIVD en de MIVD data niet zelf kunnen vergaren en een buitenlandse dienst beschikt over data die relevant zijn voor de taken van de Nederlandse diensten, kan dit worden gedeeld. Het kan daarbij – om een voorbeeld te geven – gaan om informatie die noodzakelijk is voor de beveiliging van Nederlandse militairen in het buitenland, waarbij het voor Nederland – bijvoorbeeld

wegens de geografische ligging – niet mogelijk is de relevante telecommunicatiedata, waaronder metadata, te onderscheppen door eigen inzet van de bijzondere bevoegdheden. Daarbij kan het gaan om data die door de buitenlandse dienst op verzoek van de Nederlandse dienst worden vergaard of data waarover de buitenlandse dienst reeds beschikt en die op vrijwillige basis – al dan niet in het kader van een samenwerkingsverband – met de Nederlandse dienst worden gedeeld. Bij het intercepteren van data op verzoek van de Nederlandse dienst is van belang dat de dienst aan een partner niet mag vragen om gebruik te maken van een interceptievorm die de dienst op grond van de WIV 2002 niet zou kunnen inzetten.

*Contra-inlichtingen*

3.2.13 De Nederlandse diensten verrichten contra-inlichtingen (CI)-activiteiten om te onderzoeken of buitenlandse diensten informatie vergaren op een wijze die inbreuk maakt op de Nederlandse soevereiniteit. Indien dit onderzoek leidt tot de vaststelling dat een bepaalde dienst activiteiten verricht binnen de Nederlandse rechtssfeer zonder daartoe een verzoek te hebben gedaan bij de Nederlandse diensten, worden passende maatregelen getroffen.

Zie: Toezichtsrapport CTIVD nr. 22A, p. 6 (productie 17).

*3.3 Relevante bevoegdheden van de Amerikaanse National Security Agency*

*PRISM*

3.3.1 Op grond van Section 702 FISA zijn de *Attorney General* en de *Director of National Intelligence* bevoegd voor een periode tot een jaar buitenlands inlichtingenmateriaal te vergaren over personen ten aanzien van wie het redelijke vermoeden bestaat dat zij zich buiten de Verenigde Staten bevinden. Het buitenlandse inlichtingenmateriaal wordt vergaard met of met behulp van een elektronische communicatieservice provider. Het gaat daarbij om persoonlijke informatie, zoals de inhoud van communicaties via internet, e-mail of telefoon, metadata, foto's en activiteiten op internet. Buitenlands inlichtingenmateriaal *(foreign intelligence information*) is in de wet gedefinieerd als – kort gezegd – informatie die relevant is voor de bescherming van de nationale veiligheid van de Verenigde Staten. Daarbij gaat het om internationaal terrorisme, sabotage of spionage door een buitenlandse mogendheid of een vertegenwoordiger van een buitenlandse mogendheid of om de verdediging, veiligheid of het buitenlands beleid van de Verenigde Staten (Sections 203(b)(2) en 203(d)(2) USA PATRIOT Act 2001). Alvorens de bevoegdheid ex Section 702 kan worden uitgeoefend, dient een machtiging te worden verkregen van de *United States Foreign Intelligence Surveillance Court* (hierna: FISC). Voorts gelden de volgende voorwaarden:

- De vergaring mag niet opzettelijk zijn gericht op personen van wie bekend is dat ze zich op het moment van vergaring binnen de Verenigde Staten bevinden.
- De vergaring mag niet opzettelijk zijn gericht op personen die zich buiten de Verenigde Staten bevinden, terwijl het doel van die vergaring is gericht op een persoon die zich in de Verenigde Staten bevindt.
- De vergaring mag niet opzettelijk zijn gericht op een Amerikaanse burger ten aanzien van wie het redelijk vermoeden bestaat dat hij of zij zich buiten de Verenigde Staten bevindt.
- De vergaring mag niet opzettelijk zijn gericht op het onderscheppen van communicaties waarvan bekend is dat zowel de zender als de beoogde ontvangers zich binnen de Verenigde Staten bevinden.
- De vergaring dient te worden uitgevoerd op een wijze die verenigbaar is met het Vierde Amendement van de Amerikaanse constitutie.

3.3.2 Uit de door Snowden openbaar gemaakt documenten kan worden afgeleid dat in het PRISM programma op grond van bevelen ex Section 702 buitenlands inlichtingenmateriaal wordt verwerkt, dat is verkregen van Amerikaanse providers van elektronische communicatiediensten en door het onderscheppen van internetcommunicatie die door kabels of transmissiepunten in de Verenigde Staten wordt getransporteerd. Daarbij kan het dus ook gaan om het onderscheppen van (metadata betreffende) communicatie van Nederlanders, ook als die Nederlanders zich in Nederland bevinden, voor zover die communicatie plaatsvindt via providers, kabels en/of transmissiepunten op Amerikaans grondgebied.

Zie: Council of the European Union, Report on the findings by the EU Co-chairs and the ad hoc EU-US Working Group on Data Protection, 27 November 2013, 16987/13, p. 5-6 (productie 2).

*Section 215 (FISC document production order)*

3.3.3 Amerikaanse inlichtingen- en veiligheidsdiensten, waaronder de NSA, kunnen metadata verzamelen door het uitvaardigen van een *FISC document production order.* De wettelijke basis van de *FISC document production order* betreft Section 215 van de USA PATRIOT Act van 2001 (gewijzigd in 2005). Op grond van een *FISC document production order* (hierna: Section 215 order) kan een derde partij, zoals telecommunicatieservice providers, worden verplicht de in het bevel genoemde 'tastbare zaken' te verstrekken. Het gaat daarbij om de verstrekking van metadata. Deze metadata kunnen ook betrekking hebben op Nederlanders, wier telecommunicatie plaatsvindt via een Amerikaanse telecommunicatieservice provider.

Zie:

- Council of the European Union, Report on the findings by the EU Co-chairs and the ad hoc EU-US Working Group on Data Protection, 27 November 2013, 16987/13, p. 4 (productie 2).
- Administration White Paper, Bulk Collection of Telephony Metadata under Section 215 of the USA PATRIOT Act, August 9, 2013. Beschikbaar via: http://cryptome.org/2013/08/doj-13-0809.pdf.

3.3.4 De bevoegdheid ex Section 215 kan worden ingezet in het kader van een onderzoek ter vergaring van buitenlands inlichtingenmateriaal dat niet betrekking heeft op een Amerikaanse burger of in het kader van een onderzoek naar internationaal terrorisme of spionage. Voor een bevel tot het verstrekken van de metadata is een machtiging nodig van het FISC. Een machtiging wordt door het FISC verleend indien sprake is van feiten en omstandigheden waaraan het redelijk vermoeden kan worden ontleend dat de gevraagde documenten relevant zijn voor een geautoriseerd onderzoek.

*Toezicht en controle*

3.3.5 Het gebruik van aan de NSA toekomende bevoegdheden tot het vergaren van gegevens is onderworpen aan parlementaire controle en aan het toezicht van de interne *Inspector General.* Deze controle vindt achteraf plaats. De *Intelligence Committees* en *Judiciary Committees* in het Amerikaanse congres ontvangen de geclassificeerde rapporten over de toepassing van de bevoegdheden. Voorts verstrekken de inlichtingendiensten aan het congres informatie over het aantal verzoeken tot toepassing van de betreffende bevoegdheden dat is gedaan, het aantal verzoeken dat door het FISC is geweigerd en het aantal machtigingen dat door het FISC is verleend.

Bovendien hebben onder meer de *NSA director,* de *Director of National Intelligence* en de *Inspector General of the Intelligence Community* naar aanleiding van de gelekte documenten van de NSA in hoorzittingen van het Amerikaanse congres verklaringen afgelegd over de bevoegdheden van de NSA en het gebruik van deze bevoegdheden. De *Inspector General of the Intelligence Community* is door het *Committee on the Judiciary* van de Amerikaanse Senaat gevraagd onderzoek te doen naar het gebruik van de bevoegdheden ex Section 702 FISA en Section 215 USA PATRIOT Act. Ook heeft het *Intelligence Committee* van de Amerikaanse Senaat een wetsvoorstel ingediend dat ertoe moet leiden dat het vergaren van metadata op grond van Section 215 wordt beperkt en dat privacywaarborgen en controle en toezicht op het gebruik van Section 215 order en de bevoegdheid ex Section 702 FISA worden versterkt.

3.3.6 Voorafgaand aan de inzet van de bevoegdheid ex Section 702 FISA en Section 215 van de USA PATRIOT Act vindt rechterlijke controle plaats door de FISC.

3.3.7 Het FISC heeft bij het verlenen van een machtiging voor het uitoefenen van de bevoegdheid ex Section 702 FISA beoordeeld of dit verenigbaar is met het Vierde

Amendement van de Amerikaanse Grondwet. In het Vierde Amendement wordt het recht op privacy gewaarborgd door bescherming te bieden tegen onredelijke *search* en *surveillance* activiteiten van de Amerikaanse overheid. Het FISC en het *Foreign Intelligence Surveillance Court of Review* hebben de bevoegdheid tot het vergaren van buitenlands inlichtingenmateriaal, waaronder de inhoud van communicaties, dat is gericht op personen buiten de Verenigde Staten, in beginsel in overeenstemming met het Vierde Amendement geacht. Omdat de onderschepte communicatie ook de communicaties van Amerikanen kan betreffen, dient volgens het FISC per aanvraag te worden beoordeeld of sprake is van een aanvraag die, gelet op alle omstandigheden van het geval, als redelijk moet worden aangemerkt in de zin van het Vierde Amendement.

Zie:
- *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act,* 551 F.3d 1004 (FISC of Review 2008);
- FISC October 3, 2011 (Memorandum Opinion), 2011 WL 10945618, 24-25.

In het licht van de 'redelijkheidstoets' op grond van het Vierde Amendement heeft het FISC een aanvraag voor een machtiging vanwege de toepasselijke *targeting* en *minimization* procedures niet verenigbaar geacht met het Vierde Amendement, nu deze niet konden voorkomen dat een groot aantal communicaties van Amerikaanse burgers werd onderschept. *Targeting* en *minimization* procedures dienen ertoe te leiden dat onderschepte informatie die niet voldoet aan de wettelijke voorwaarden van Section 702 FISA en aan de voorwaarden neergelegd in de machtiging van de FISC, worden verwijderd. Omdat de betreffende procedures hieraan niet voldeden, werd de machtiging op dat moment niet verleend. De *Director of National Intelligence* werd door het FISC in de gelegenheid gesteld de *targeting* en *minimization* procedures aan te passen.

Zie: FISC October 3 (Memorandum Opinion), 2011, 2011 WL 10945618, 24-25).

3.3.8 Bij de beoordeling van een aanvraag voor het verstrekken van metadata van telefoongesprekken 'in bulk' door een telecommunicatieservice provider, heeft het FISC geoordeeld dat een dergelijke aanvraag in overeenstemming is met het Vierde Amendement van de Amerikaanse constitutie. Van belang daarbij is dat volgens vaste rechtspraak van het *Supreme Court* geen sprake is van een redelijke verwachting van privacy ten aanzien van metadata (zie: *Smith v. Maryland,* 99 S.Ct. 2577 (1979)). Voorts is geen sprake van een redelijke verwachting van privacy ten aanzien van metadata vrijwillig verstrekt aan een derde partij (zie: *United States v. Miller,* 96 S.Ct. 1619 (1976)). In het licht van deze vaste rechtspraak oordeelde het FISC dat de aanvraag voor de machtiging tot het verstrekken van metadata van telefoongesprekken, niet in strijd is met het Vierde Amendement, ook niet als het gaat om de brede vergaring van metadata op grond van één machtiging.

Zie: *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted],* Amended Memorandum opinion, FISC 29 August 2013, WL6741573, 1-3.

Het FISC oordeelde vervolgens dat de aanvraag eveneens in overeenstemming was met de daarvoor geldende wettelijke vereisten, waarom de machtiging is verleend.

Zie voorts: *United States v. Moalin,* 2013 WL 6079518 (S.D.Cal. 2013).

3.3.9 Voorts is de rechtmatigheid van de betreffende bevoegdheden van (onder meer) de NSA in civiele procedures aangespannen door mensenrechtenorganisaties als Amnesty International en de American Civil Liberties Union en door een collectief van consumenten van telecommunicatie- en internetproviders ter discussie gesteld.

3.3.10 Amnesty International USA en anderen hebben na de inwerkingtreding van Section 702 FISA op grond van de FISA Amendments Act of 2008 de *Director of National Intelligence* in rechte betrokken om een verklaring voor recht te verkrijgen dat Section 702 FISA en enige vergaring die op basis van deze bepaling is geautoriseerd in strijd is met de Amerikaanse constitutie. Volgens de eisende partijen hadden zij belang bij een dergelijke verklaring voor recht, omdat objectief gezien sprake zou zijn van een redelijke mate van waarschijnlijkheid dat op enig moment op grond van Section 702 FISA hun communicaties zouden worden onderschept. Het *Supreme Court* heeft op 26 februari 2013 de eisende partijen niet-ontvankelijk verklaard wegens de speculatieve aard van de vordering. De eisende partijen hebben naar het oordeel van het *Supreme Court* niet aannemelijk kunnen maken dat het door hen gestelde nadeel daadwerkelijk zal optreden.

Zie: *Clapper v. Amnesty International USA et al,* 133 S.Ct. 1138 (2013) (**productie 18**).

3.3.11 Ook ten aanzien van het intercepteren van metadata in bulk op grond van section 215 zijn inmiddels verschillende civiele procedures aanhangig gemaakt bij federale rechtbanken.

3.3.12 Op 16 december 2013 heeft de *district judge* van het *United States District Court for the District of Columbia* de Amerikaanse overheid verboden metadata te vergaren op grond van Section 215 die verband houden met de Verizon abonnementen van de eisers in deze zaak en bevolen metadata die in bulk door de overheid zijn vergaard te vernietigen. Volgens deze *district judge* is de uitspraak van het *Supreme Court* in *Smith v. Maryland* (1979) achterhaald gelet op de huidige technische mogelijkheden en is de vergaring van metadata in bulk betreffende telefoonverkeer in strijd met het Vierde Amendement. De betreffende rechter heeft daarbij bepaald dat in afwachting

van een oordeel in hoger beroep aan deze uitspraak door de Amerikaanse overheid geen uitvoering hoeft te worden gegeven.

> Zie: *Klayman et al. v. Obama,* no. 13-0851 (D.D.C. 2013) (**productie 19**).

3.3.13 De *district judge* van het *United States District Court Southern District of New York* kwam op 27 december 2013 tot een ander oordeel. Naar het oordeel van deze *district judge* en onder verwijzing naar het oordeel van het *Supreme Court* in *Smith v. Maryland,* is de vergaring door de NSA van metadata in bulk betreffende telefoonverkeer rechtmatig en in het licht van het Vierde Amendement een redelijke methode ter bescherming van de nationale veiligheid. De vordering van de *American Civil Liberties Union* en anderen is dan ook afgewezen.

> Zie: *American Civil Liberties Union et al. v. James R. Clapper et al.,* no. 13-Civ, 3994 (WHP) (S.D.N.Y. 2013) (**productie 20**).

3.3.14 President Obama heeft op 17 januari 2014 een aantal hervormingen aangekondigd van de bevoegdheden waarvan de NSA gebruik maakt. Deze hervormingen betreffen onder meer een beperking en preciezere afbakening van de doelen waarvoor metadata in bulk kunnen worden vergaard en een vergroting van de transparantie en versterking van het toezicht bij de uitoefening van de bevoegdheden door de NSA. Voorts dienen de hervormingen te leiden tot een versterking van privacywaarborgen voor zowel Amerikanen als niet-Amerikanen.

> Zie: Presidential Policy Directive/PPD-28, January 17, 2014. Beschikbaar via: http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>

## 4 Juridisch kader

*Eisen aan het vergaren en verwerken van inlichtingen die voortvloeien uit het recht op bescherming van de persoonlijke levenssfeer (artikel 8 EVRM)*

4.1 Het recht op bescherming van de persoonlijke levenssfeer is gewaarborgd in artikel 8 Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (hierna: EVRM). Artikel 8 EVRM bepaalt als volgt:

> "1. Een ieder heeft recht op respect voor zijn privé leven, 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."

Het recht op bescherming van de persoonlijke levenssfeer wordt ook gewaarborgd in artikel 10 van de Grondwet, artikel 17 van het Internationaal Verdag inzake Burgerrechten en Politieke Rechten en in de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie. Nu het recht op bescherming van de persoonlijke levenssfeer op grond van deze bepalingen wordt uitgelegd aan de hand van de rechtspraak van het Europees Hof voor de Rechten van de Mens over artikel 8 EVRM, worden deze bepalingen verder niet besproken.

4.2 Op grond van vaste jurisprudentie van het Europees Hof voor de Rechten van de Mens (hierna: EHRM) beschermt artikel 8 EVRM het individu tegen willekeurige inbreuken door de overheid op zijn of haar persoonlijke levenssfeer. Daarbij komt de lidstaten beoordelingsvrijheid toe bij het maken van een afweging tussen de botsende belangen van het individu enerzijds en van de (bescherming van de) samenleving als geheel anderzijds.

Zie:
- EHRM 27 oktober 1994, app. no. 18535/91 (*Kroon and Others v. The Netherlands,* par. 31;
- EHRM 24 juni 2004, app. No. 59320/00 (*Von Hannover v. Germany*), par. 31 en 57.

4.3 In de rechtspraak van het EHRM wordt het concept 'persoonlijke levenssfeer' breed uitgelegd. Het omvat de fysieke en psychologische integriteit en aspecten die verband houden met de identiteit van een persoon. Daarbij kan het gaan om activiteiten die plaatsvinden in het privéleven, het professionele leven en in het openbaar waar sprake is van een *'zone of interaction'* met andere personen.

Zie:
- EHRM 24 juni 2004, app. No. 59320/00 (*Von Hannover v. Germany*), par. 50;
- EHRM 25 september 2001, app. No. 44787/98 (*P.G. and J.H. v. The United Kingdom*), par. 56;
- EHRM 25 oktober 2007m app. No. 38258/03 (*Van Vondel v. The Netherlands*), par. 48;
- EHRM 2 september 2010, app. no. 35623/05 (*Uzun v. Germany*), par. 43.

Dit betekent dat ook het onderscheppen en verwerken van metadata onder de reikwijdte van artikel 8 EVRM valt.

Zie:
- EHRM 2 augustus 1984, app. no. 8691/79 (*Malone v. The United Kingdom*), par. 84:

> "The records of metering contain information, in particular the number dialed, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8 (art. 8)."

Zie voorts:
- EHRM 25 september 2001, app. No. 44787/98 (*P.G. and J.H. v. The United Kingdom*), par. 42.

Hetzelfde geldt voor het opslaan en verwerken van persoonlijke gegevens.

Zie:
- EHRM 26 maart 1987, app. no. 9248/81 (*Leander v. Sweden*), par. 48;
- EHRM 16 februari 2000, app. no. 27798/95 (*Amann v. Switzerland*), par. 65 en 69;
- EHRM 4 mei 2000, app. no. 28341/95 (*Rotaru v. Romania*), par. 46.

4.4 Volgens vaste rechtspraak van het EHRM is een ingreep in de persoonlijke levenssfeer van een individu op grond van het tweede lid van artikel 8 EVRM gerechtvaardigd indien die ingreep in overeenstemming is met het recht en noodzakelijk is in de democratische samenleving voor de verwezenlijking van een van de in artikel 8 lid 2 EVRM genoemde doelen. Een ingreep in de persoonlijke levenssfeer is in overeenstemming met het recht indien er sprake is van een basis in het nationale recht (in Nederland gelet op artikel 10 Grondwet een wet in formele zin) die (i) toegankelijk is en (ii) met voldoende precisie is geformuleerd in de zin dat eenieder kan voorzien in welke situaties de autoriteiten mogen ingrijpen in de persoonlijke levenssfeer (voorzienbaarheid).

Zie:
- EHRM 26 april 1979, app. no. 6538/74 (*Sunday Times v. The United Kingdom*), par. 49;
- EHRM 24 april 1990, app. nos. 11801/85 en 11105/84 (*Kruslin v. France* en *Huvig v. France*), par. 30/29;
- EHRM 2 augustus 1984, app. no. 8691/79 (*Malone v. The United Kingdom*), par. 66;
- EHRM 2 september 2010, app. no. 35623/05 (*Uzun v. Germany*), par. 60-61.

De ingreep wordt geacht noodzakelijk te zijn in een democratische samenleving voor een van de in artikel 8 lid 2 genoemde doelen indien de ingreep beantwoordt aan een dringende maatschappelijke behoefte (*pressing social need*) en proportioneel is om het beoogde doel te realiseren.

Zie:

- EHRM 25 maart 1983, app. nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 en 7136/75 (*Silver and others v. The United* Kingdom), par. 97;
- EHRM 26 maart 1987, app. no. 9248/81 (*Leander v. Sweden*), par. 58.

4.5 Voor heimelijke *surveillance* methoden geldt dat de basis in de wet voldoende voorzienbaar is indien die basis een adequate en effectieve waarborg biedt tegen willekeurige ingrepen op de persoonlijke levenssfeer. Wat daar in het concrete geval onder wordt verstaan, is afhankelijk van onder meer de aard, reikwijdte en duur van de toegepaste bevoegdheid, de redenen voor de toepassing, de verantwoordelijke autoriteiten en de toepasselijke waarborgen in het nationale recht.

Zie bijvoorbeeld:
- EHRM 2 september 2010, app. no. 35623/05 (*Uzun v. Germany*), par. 63.

4.6 In dat verband onderscheidt het EHRM uitdrukkelijk het vergaren van metadata van het vergaren van de inhoud van communicaties.

Zie:
- EHRM 2 augustus 1984, app. no. 8691/79 (*Malone v. The United Kingdom*), par. 84:

"By its very nature, metering is therefore to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified. The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes cannot give rise to an issue under Article 8 (art. 8)."

Vergelijk voorts:
- EHRM 25 september 2011, app. no 44787/98 (*P.G. and J.H. v. The United Kingdom*), par. 42.

Het EHRM stelt hogere eisen waar het gaat om het afluisteren van (tele)communicatie dan aan heimelijke bevoegdheden die in mindere mate ingrijpen op de persoonlijke levenssfeer, zoals het vergaren van metadata. Voor het vergaren van metadata dient de basis in het recht een adequate en effectieve bescherming te bieden tegen willekeurige inbreuken op de persoonlijke levenssfeer. De basis in het recht voor het afluisteren van (tele)communicatie dient naar het oordeel van het EHRM in het bijzonder precies te zijn en recht te doen aan bepaalde door het EHRM geformuleerde minimumwaarborgen.

Zie:
- EHRM 24 april 1990, app. nos. 11801/85 en 11105/84 (*Kruslin v. France* en *Huvig v. France*), par. 33/32;

In de ontvankelijkheidsbeslissing *Weber and Saravia v. Germany,* heeft het EHRM de in eerdere rechtspraak voor het afluisteren van communicatie aanvullende minimumwaarborgen samengevat. Zie: EHRM 29 juni 2006, app, no. 54934/00 (*Weber and Saravia v. Germany*) (ontvankelijkheidsbeslissing), par. 95.

De eisen die worden gesteld aan het vergaren van metadata of aan andere minder ingrijpende bevoegdheden, zijn van een andere aard.

Zie bijvoorbeeld: EHRM 2 september 2010, app. no. 35623/05 (*Uzun v. Germany*), par. 61, 63, 65 en 66 (in deze zaak werd GPS surveillance en observatie van personen in openbare ruimtes als een minder vergaande ingreep op de persoonlijke levenssfeer aangemerkt, waarom het EHRM minder eisen stelt aan de 'voorzienbaarheid' van de basis van de ingreep):

"While the Court is not barred from gaining inspiration from these principles, it finds that these rather strict standards, set up and applied in the specific context of surveillance of telecommunications [...], are not applicable as such to cases such as the present one, concerning surveillance via GPS of movements in public places and thus a measure which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations [...]. It will therefore apply the more general principles on adequate protection against arbitrary interference with Article 8 rights as summarised above (see paragraph 63).

Zie voorts: EHRM 25 september 2011, app. no 44787/98 (*P.G. and J.H. v. The United Kingdom*), par. 46:

"The Court observes that the quality of the law criterion in this context refers essentially to considerations of foreseeability and lack of arbitrariness [...]. What is required by way of safeguard will depend, to some extent at least, on the nature and extent of the interference in question. In this care, the information obtained concerned the telephone number called from B.'s flat between two specific dates. It did not include any information about the contents of those calls, or who made or received them. The data obtained, and the use that could be made of them, were therefore strictly limited."

4.7 Voorts neemt het EHRM in aanmerking dat het voorzienbaarheidsvereiste niet met zich kan brengen dat een persoon in staat moet zijn te voorzien wanneer zijn communicatie wordt afgeluisterd, nu dat zou betekenen dat het gedrag daarop kan worden afgestemd. Het gaat erom dat op grond van de basis in de wet voorzienbaar is in welke omstandigheden en onder welke voorwaarden de overheid geheime onderzoeksbevoegdheden mag inzetten.

Zie:

- EHRM 2 augustus 1984, app. no. 8691/79 (*Malone v. The United Kingdom*), par. 67;

- EHRM 24 april 1990, app. nos. 11801/85 en 11105/84 (*Kruslin v. France* en *Huvig v. France*), par. 30/29.
- EHRM 29 juni 2006, app, no. 54934/00 (*Weber and Saravia v. Germany*) (ontvankelijkheidsbeslissing), par. 95;
- EHRM 2 september 2010, app. no. 35623/05 (*Uzun v. Germany*), par. 63;
- EHRM 22 november 2012, app. no. 39315/06 (*Telegraaf Media Nederland Landelijke Media B.V. and others v. The Netherlands*), par. 90.

4.8 In *Klass and others v. Germany* heeft het EHRM bovendien geoordeeld dat, gelet op het heimelijke karakter van *surveillance* methoden, niet is vereist dat de inzet van de bevoegdheid is onderworpen aan de controle door een rechter. Andere methoden van toezicht en controle, zoals parlementaire controle en intern toezicht, kunnen voldoende zijn. Dit betekent evenmin dat de autoriteiten gehouden zijn na afloop van de *surveillance* de betrokkenen te notificeren. Naar het oordeel van het EHRM is een dergelijke verplichting praktisch onuitvoerbaar. Een absolute notificatieverplichting is – aldus het EHRM – bovendien niet te verenigen met het tweede lid van artikel 8 EVRM, nu het de effectiviteit van de surveillance zal ondermijnen.

Zie: EHRM 6 september 1978, app. no. 5029/71 (*Klass and Others v. Germany*), par. 58.

4.9 Tot slot is van belang dat het EHRM uitgaat van een grotere mate van beoordelingsvrijheid voor lidstaten waar het gaat om de toepassing van methoden voor de bescherming van de nationale veiligheid. De eisen die in dat geval worden gesteld aan de voorzienbaarheid van de wettelijke basis voor de bevoegdheid zijn lager.

Zie:
- EHRM 6 september 1978, app. no. 5029/71 (*Klass and Others v. Germany*), par. 48;
- EHRM 29 juni 2006, app, no. 54934/00 (*Weber and Saravia v. Germany*) (ontvankelijkheidsbeslissing), par. 106.

*Positieve verplichting op grond van artikel 8 EVRM*

4.10 Het EHRM heeft op grond van artikel 8 EVRM ook de positieve verplichting van de lidstaten aangenomen het in het eerste lid van artikel 8 EVRM gewaarborgde recht te effectueren.

Zie bijvoorbeeld: EHRM 17 juli 20013, app. no. 25337/94 (*Craxi (no. 2) v. Italy*), par. 73:

"Nevertheless, the Court recalls that while the essential object of Article 8 is to protect the individual against arbitrary interferences by the public

authorities, it does not merely compel the State to abstain from such interference: in addition to this negative undertaking, there may be positive obligations inherent in effective respect for private life."

4.11 Om vast te stellen of in een concreet geval sprake is van een positieve verplichting dient te worden beoordeeld of sprake is van een redelijke balans tussen de algemene belangen van de samenleving en de belangen van het individu. Daarbij geldt – net als bij de negatieve verplichting ingevolge artikel 8 EVRM – dat lidstaten bij het afwegen van die belangen een zekere mate van beoordelingsvrijheid toekomt. De doelen die zijn genoemd in het tweede lid van artikel 8 EVRM – zoals het beschermen van de nationale veiligheid – kunnen daarbij bovendien een rol spelen.

Zie: EHRM 15 maart 2012, app. no. 4149/04 en 41029/04 (*Aksu v. Turkey*), par. 62:

"The boundary between the State's positive and negative obligations under Article 8 does not lend itself to precise definition. The applicable principles are, nonetheless, similar. In both contexts, regard must be had to the fair balance that has to be struck between the competing interests of the individual and of the community as a whole; and in both contexts the State enjoys a certain margin of appreciation [...]."

EHRM 18 juni 2013, app. no. 50474/08 (*Bor v. Hungary*), par. 24:

"Furthermore, even in relation to the positive obligations flowing from the first paragraph of Article 8, in striking the required balance the aims mentioned in the second paragraph may be of a certain relevance [...]."

4.12 Het EHRM beoordeelt pas of sprake is van een positieve verplichting, indien sprake is van een concrete inbreuk op het recht op persoonlijke levenssfeer. Een positieve verplichting die ziet op het treffen van maatregelen om te voorkomen dat een inbreuk op het recht op bescherming van de persoonlijke levenssfeer zal plaatsvinden, kan niet uit de jurisprudentie van het EHRM worden afgeleid. Net zoals voor het aannemen van een positieve verplichting op grond van artikel 2 EVRM tot het treffen van maatregelen ter bescherming van het recht op leven, dient voor het aannemen van een positieve verplichting ex artikel 8 EVRM sprake te zijn van een daadwerkelijk en onmiddellijk gevaar voor schending van het recht op bescherming van de persoonlijke levenssfeer. Een in algemene termen gestelde mogelijke (toekomstige) schending is daarvoor onvoldoende.

EHRM 28 oktober 1998, 87/1997/871/1083, (*Osman v. The United Kingdom*), par. 128:

"The Court recalls that it has not found it established that the police knew or ought to have known at the time that Paget-Lewis represented a real and

immediate risk to the life of Ahmet Osman and that their response to the events as they unfolded was reasonable in the circumstances and not incompatible with the authorities' duty under Article 2 of the Convention to safeguard the right to life. In the Court's view, that conclusion equally supports a finding that there has been no breach of any positive obligation implied by Article 8 of the Convention to safeguard the second applicant's physical integrity."

Zaken waarin het EHRM heeft geoordeeld dat een lidstaat maatregelen had moeten treffen om de inbreuk te voorkomen, betreffen met name het effectueren van het recht op familieleven in een concreet geval (zoals gezinshereniging) of het (nalaten van het) treffen van maatregelen om bijvoorbeeld geluidshinder tegen te gaan. In de zaak *Craxi (no. 2) v. Italy* werd een schending van de positieve verplichting onder artikel 8 EVRM aangenomen doordat de overheid onvoldoende maatregelen had getroffen om te voorkomen dat afgeluisterde telefoongesprekken waarover het openbaar ministerie beschikte waren uitgelekt naar de pers (EHRM 17 juli 20013, app. no. 25337/94, par. 74-76).

## 5 Ontvankelijkheid

5.1 In deze procedure treden negen eisers op, waaronder vijf natuurlijke personen en vier rechtspersonen. In onderdeel 7 van de dagvaarding wordt gesteld dat eisers in deze procedure allemaal een bijzonder belang hebben om zich tegen de praktijken van de NSA en andere buitenlandse inlichtingendiensten te verzetten. Het betoog van de natuurlijke personen komt er kort gezegd op neer dat zij door buitenlandse inlichtingendiensten, meer specifiek de NSA, zouden kunnen worden getapt. Dat wordt niet nader toegelicht en geconcretiseerd.

5.2 De stellingen zijn op dit punt zo algemeen en onbepaald van aard, en bovendien zodanig speculatief, terwijl ook geen concreet verband wordt gelegd met het onrechtmatig handelen dat eisers de Staat verwijten en met de vorderingen die zij op basis daarvan formuleren, en die zien op handelen van de Staat, dat moet worden geconcludeerd dat deze eisers geen voldoende, concreet en eigen belang bij de vorderingen hebben. Zij moeten daarin op die grond niet-ontvankelijk worden verklaard.

5.3 Naast de eisers/natuurlijke personen treden vier rechtspersonen als eisers op. Ook het belang dat deze eisers bij de vorderingen stellen te hebben wordt slechts in algemene bewoordingen omschreven, terwijl ook hier de relatie met het onrechtmatig handelen dat eisers de Staat verwijten en met de vorderingen die zij op basis daarvan formuleren en die zien op handelen van de Staat ontbreekt. Dat geldt in de eerste plaats voor de eisers sub 6 en 7, de NVSA en de NVJ. De belangen die deze verenigingen zich blijkens hun doelstellingen aantrekken zijn andere dan de belangen

waarin zij in deze procedure bescherming zoeken. Ook zij moeten daarom niet-ontvankelijk worden verklaard in hun vorderingen. Van eiser sub 8, Internet Society Nederland, is niet gesteld dat deze rechtspersoonlijkheid heeft, zodat Internet Society Nederland op deze grond niet in zijn vorderingen kan worden ontvangen. Ten aanzien van eiseres sub 9, Stichting Privacy First, wil de Staat aannemen dat zij een voldoende belang heeft, ook al ontbreekt ook bij deze eiser een toelichting waarin een verband wordt gelegd met de vorderingen.

5.4 Dit betekent dat alleen Stichting Privacy First in haar vorderingen kan worden ontvangen. Dat geldt evenwel niet voor vordering III, die erop neerkomt dat "degenen wier belangen zij ingevolge hun statuten behartigen" – dat wil zeggen iedereen - kort gezegd moeten worden geïnformeerd over onrechtmatige gegevensverwerking en dat hen betreffende gegevens moeten worden gewist. Met deze vordering wordt eraan voorbij gezien dat in (artikel 47 e.v. van) de WIV 2002 een kennisnemingsregeling is opgenomen. Tegen onwelgevallige besluiten op verzoeken om kennisneming staat bestuursrechtelijke rechtsbescherming open, hetgeen bemoeienis van de civiele rechter uitsluit. Op die grond moet ook de Stichting Privacy First niet-ontvankelijk worden verklaard in vordering III in al haar onderdelen.

## 6 Reactie op de stellingen in de dagvaarding

6.1 In het voorgaande is een groot deel van de door eisers in de dagvaarding ingenomen stellingen reeds weersproken. In het navolgende zal de Staat de meest in het oog springende stellingen nog afzonderlijk bespreken. Voor zover daarbij enige stelling onbesproken zou blijven, mag daaruit niet worden afgeleid dat de Staat die stelling zou onderschrijven.

6.2 Eisers baseren hun vorderingen voor het belangrijkste deel op krantenartikelen. Die artikelen geven geen goed beeld van de werkelijkheid. Zo wordt in de artikelen, onder verwijzing naar een document van de NSA, gesproken van 1,8 miljoen "gesprekken" die door de NSA zouden zijn "afgeluisterd" en door de NSA aan Nederlandse inlichtingendiensten zouden zijn verstrekt. Op die "feiten" worden vervolgens de vorderingen gebaseerd. In werkelijkheid gaat het hierbij niet om gesprekken, maar om metadata, die door de Staat in het kader van de internationale samenwerking rechtmatig zijn verkregen en rechtmatig aan andere landen zijn verstrekt. Hieruit blijkt dat de betreffende krantenartikelen geen goede basis voor de vaststelling van de relevante feiten kunnen vormen.

6.3 Eisers stellen dat de Amerikaanse NSA gegevens vergaart in strijd met artikel 8 EVRM. De Amerikaanse FISA zou volgens eisers niet voldoen aan de vereisten die het EHRM op grond van artikel 8 EVRM heeft gesteld aan het toepassen van methoden van *surveillance*. Deze stelling van eisers kan niet slagen. De Verenigde Staten zijn geen partij bij het EVRM. Evenmin kan Nederland aansprakelijk – gelet op het voorgaande is

van aansprakelijkheid geen sprake – worden gehouden voor schendingen van het EVRM door de Verenigde Staten.

6.4 Op grond van artikel 1 EVRM verzekeren de Verdragsluitende partijen eenieder die ressorteert onder hun rechtsmacht, de rechten en vrijheden die zijn vastgesteld in de Eerste Titel van het Verdrag. Dit betekent dat het EVRM niet van toepassing is op staten die geen partij zijn bij het EVRM en voorts dat Verdragsstaten niet zijn gehouden standaarden ontleend aan het EVRM aan andere staten op te leggen.

> Dit uitgangspunt heeft slechts uitzondering in het geval een uitlevering of uitzetting vanuit een Verdragsstaat leidt tot schending van artikel 2 en/of 3 EVRM en, in uitzonderlijke gevallen, van artikel 5 en/of 6 EVRM in de om uitlevering verzoekende staat, respectievelijk in de staat waarnaar wordt uitgezet.
>
> Zie:
> - EHRM 7 juli 1989, *Soering v. The United Kingdom,* app. no. 14038/88, par. 86;
> - EHRM 12 december 2011, *Banković and others v. Belgium and others,* app. no. 52207/99 (ontvankelijkheidsbeslissing), par. 67-68:
>
> "67. In keeping with the essentially territorial notion of jurisdiction, the Court has accepted only in exceptional cases that acts of the Contracting States performed, or producing effects, outside their territories can constitute an exercise of jurisdiction by them within the meaning of Article 1 of the Convention.
> 68. Reference has been made in the Court's case-law, as an example of jurisdiction "not restricted to the national territory" of the respondent State [...], to situations where the extradition or expulsion of a person by a Contracting State may give rise to an issue under Articles 2 and/or 3 (or, exceptionally, under Articles 5 and or 6) and hence engage the responsibility of that State under the Convention [...].
> However, the Court notes that liability is incurred in such cases by an action of the respondent State concerning a person while he or she is on its territory, clearly within its jurisdiction, and that such cases do not concern the actual exercise of a State's competence or jurisdiction abroad [...]."

6.5 Zoals toegelicht (zie randnummers 3.3.5-3.3.14) kennen de Verenigde Staten hun eigen systeem van toezicht en controle op de wijze waarop de NSA informatie vergaart. Het Vierde Amendement van de Amerikaanse Grondwet biedt bescherming tegen onredelijke inbreuken op de persoonlijke levenssfeer door het toepassen van *surveillance* bevoegdheden door de Amerikaanse overheid. Bovendien zijn de Verenigde Staten partij bij het IVBPR.

6.6 Voorts stellen eisers dat de Staat artikel 8 EVRM schendt door gebruik te maken van gegevens verkregen van de Amerikaanse NSA. De Staat begrijpt dat het daarbij gaat

om het gebruik van gegevens verkregen door toepassing van de bevoegdheden ex Section 702 FISA en Section 215 van de USA PATRIOT Act. Zoals gezegd zijn de Nederlandse inlichtingendiensten niet bekend met de wijze waarop door buitenlandse inlichtingendiensten verstrekte informatie is verkregen (zie randnummers 2.8-2.9. 2.13 en 3.1.5). Reeds daarom kan deze stelling van eisers niet slagen.

6.7 Overigens merkt de Staat op dat het in onderhavige zaak gaat om het verstrekken van metadata door de NSA aan Nederlandse inlichtingendiensten. Anders dan eisers stellen, gelden voor de vergaring van metadata niet de minimumwaarborgen die in de ontvankelijkheidsbeslissing *Weber and Saravia v. Germany* (2006) zijn geformuleerd. Deze minimumwaarborgen heeft het EHRM geformuleerd in verband met het afluisteren van communicatie van individuen, waarbij het niet gaat om het feit dát er communicatie heeft plaatsgevonden, maar wat de *inhoud* van die communicatie is geweest. Dat is een veel verdergaande ingreep op de persoonlijke levenssfeer.

6.8 Volgens eiser zou uit het arrest *Liberty v. United Kingdom* (2008) volgen dat deze waarborgen ook voor het ongericht vergaren van metadata geldt, nu het EHRM in dat arrest heeft geoordeeld dat dezelfde eisen dienen te worden gesteld aan een systeem van *strategic monitoring*. Ook deze *strategic monitoring* betrof echter het strategisch monitoren van (de inhoud van) *communicatie*. Zoals toegelicht onder randnummer 4.6, acht het EHRM het vergaren en verwerken van metadata als een lichtere ingreep op de persoonlijke levenssfeer dan het afluisteren van (tele)communicatie. De minimumwaarborgen zoals geformuleerd in *Weber and Saravia* gelden dan ook niet voor een systeem voor het vergaren van metadata.

6.9 Ook de verwerking van gegevens verkregen van buitenlandse inlichtingendiensten door de AIVD en de MIVD is, anders dan eisers stellen, niet in strijd met de WIV 2002 en/of artikel 8 EVRM. De verwerking van gegevens vindt plaats op grond van de artikelen 12 tot en met 16 van de WIV 2002. Artikel 12 WIV 2002 bepaalt dat gegevens alleen worden verwerkt voor zover noodzakelijk voor de uitvoering van de in artikelen 6 en 7 genoemde taken van respectievelijk de AIVD en MIVD. In artikel 13 van de WIV 2002 zijn de categorieën van personen genoemd ten aanzien van wie gegevens kunnen worden verwerkt. Deze regeling voldoet aan de eisen die artikel 8 EVRM stelt aan een basis in de wet voor het opslaan en de verwerking van persoonlijke gegevens.

> Vergelijk bovendien EHRM 25 september 2011, app. no 44787/98 (*P.G. and J.H. v. The United Kingdom*), par. 47-48, waaruit eveneens volgt dat de vereisten die worden gesteld aan de opslag en verwerking van metadata niet op één lijn kunnen worden gesteld met de eisen die het EHRM stelt aan het vergaren en verwerken van communicaties:
>
> "47. While it does not appear that there are any specific statutory provisions (as opposed to internal policy guidelines) governing storage and destruction

> of such information, the Court is not persuaded that the lack of such detailed formal regulation raises any risk of arbitrariness or misuse. Nor is it apparent that there was any lack of foreseeability. Disclosure to the police was permitted under the relevant statutory framework where necessary for the purposes of the detection and prevention of crime, and the material was used at the applicants' trial on criminal charges to corroborate other evidence relevant to the timing of telephone calls. It is not apparent that the applicants did not have an adequate indication as to the circumstances in, and conditions on, which the public authorities were empowered to resort to such a measure.
> 48. The Court concludes that the measure in question was "in accordance with the law"."

6.10 Eisers stellen voorts dat de Staat burgers over wie gegevens zijn ontvangen van buitenlandse inlichtingendiensten die in strijd met artikel 8 of 10 EVRM zouden zijn vergaard, hierover zou moeten informeren. Zoals gezegd weet de Staat niet op welke wijze gegevens zijn vergaard die door buitenlandse inlichtingendiensten aan de AIVD of de MIVD in het kader van een samenwerkingsrelatie worden verstrekt. Op grond van artikel 47 WIV 2002 kan eenieder bovendien een aanvraag bij de betrokken Minister indienen of en, zo ja, welke hem betreffende persoonsgegevens door of ten behoeve van een dienst zijn verwerkt. De Minister beoordeelt op grond van artikel 53 WIV 2002 of een dergelijke aanvraag kan worden ingewilligd. Dit zal in ieder geval niet gebeuren indien de gegevens betreffende de aanvrager van belang zijn voor een onderzoek van een van de diensten. Zoals toegelicht onder randnummer 4.8, kan evenmin uit artikel 8 EVRM een verplichting tot notificatie worden afgeleid.

> In artikel 34 WIV 2002 is bovendien de verplichting opgenomen tot notificatie van personen ten aanzien van wie de AIVD of MIVD een bijzondere bevoegdheid als bedoeld in de artikelen 23 lid 1, 25 lid 1, 27 lid 3 onder a en b of 30 lid 1 WIV 2002 heeft toegepast. Notificatie kan op grond van artikel 34 lid 7 WIV 2002 achterwege blijven indien dit leidt tot onthulling van de bronnen van een dienst, waaronder begrepen een buitenlandse dienst, indien door notificatie betrekkingen met andere landen en met internationale organisaties worden geschaad of indien dit leidt tot onthulling van een specifieke toepassing van een methode van een dienst of van de identiteit van een persoon die de dienst behulpzaam is geweest bij toepassing van de methode.

6.11 Evenmin is sprake van schending van een positieve verplichting uit hoofde van artikel 8 EVRM. Volgens eisers heeft de Staat artikel 8 EVRM geschonden door na te laten maatregelen te treffen ter bescherming van de persoonlijke levenssfeer in verband met de door eisers gestelde schending van artikel 8 EVRM door de wijze van vergaring van inlichtingen door de Amerikaanse NSA. Ook ten aanzien van deze stelling stelt de Staat voorop dat hij niet bekend is met de methoden waarmee inlichtingen zijn vergaard die buitenlandse inlichtingendiensten verstrekken aan de AIVD en/of de MIVD. Gelet op de reikwijdte van het EVRM (zie randnummer 6.4) is ook geen sprake

van een verplichting voor de Staat zich van de wijze van vergaring door buitenlandse diensten te vergewissen. Evenmin is sprake van een concrete inbreuk op het recht op bescherming van de persoonlijke levenssfeer door het ontvangen en eventueel verwerken van door de NSA verstrekte informatie, die een verplichting voor de Staat met zich kan brengen maatregelen te treffen om deze inbreuk te voorkomen. Van een daadwerkelijk of onmiddellijk gevaar voor schending van het recht op de persoonlijke levenssfeer is geen sprake. De door eisers gestelde aannemelijkheid, gebaseerd op berichten in de media, van een vergaring in de Verenigde Staten die in strijd is met het recht op privacy zoals dat in Nederland wordt gewaarborgd, is daarvoor hoe dan ook onvoldoende. De conclusie is dat ook de stelling van eisers dat de Staat een uit artikel 8 EVRM voortvloeiende positieve verplichting heeft geschonden niet kan slagen.

6.12 Tot slot merkt de Staat op dat evenmin sprake is van schending van de vrijheid van meningsuiting van eisers zoals gewaarborgd in artikel 10 EVRM. Eisers hebben aan hun vorderingen ook schending van artikel 10 EVRM ten grondslag gelegd. Nu volgens eisers sprake is van vergaring in strijd met het recht op bescherming van artikel 8 EVRM, zou eveneens sprake zijn van een schending van de communicatievrijheid als gewaarborgd in artikel 10 EVRM (en artikel 11 van het Handvest). Gelet op hetgeen hiervoor is opgemerkt over de door eisers gestelde schending van artikel 8 EVRM, is evenmin sprake van schending van artikel 10 EVRM.

## 7 Bespreking van de vorderingen / uitvoerbaarverklaring bij voorraad / dwangsom

7.1 Eisers hebben een uitvoerig petitum geformuleerd, met – naast een vordering tot veroordeling van de Staat in de proceskosten - drie vorderingen, waarvan de derde vordering op haar beurt drie onderdelen bevat, welke eis bij akte houdende wijziging van eis is aangevuld met de vordering aan toewijzing een dwangsom te verbinden. De conclusie op grond van het voorgaande is dat van onrechtmatig handelen van de Staat als door eisers bedoeld in het geheel geen sprake is, zodat de vorderingen moeten worden afgewezen. In het voorgaande, onderdeel 2, heeft de Staat bovendien in het bijzonder toegelicht welke verstrekkende consequenties toewijzing van de vorderingen voor de internationale samenwerking zou hebben en waardoor de diensten hun taken in het belang van de nationale veiligheid niet meer adequaat zouden kunnen uitoefenen. Het laat ook zien dat toewijzing het stelsel van bescherming van de nationale veiligheid volledig zou doorkruisen. Ook dat staat aan toewijzing in de weg.

7.2 De verstrekkendheid van de gevolgen van toewijzing en het principiële karakter ervan maken dat de Staat de rechtbank vraagt het vonnis, als daarin enigerlei vordering zou worden toegewezen, niet bij voorraad uitvoerbaar te verklaren, opdat de Staat in de gelegenheid zal zijn een voor de huidige werkwijze negatief oordeel eerst aan een hogere rechter voor te leggen zonder die werkwijze te hoeven aanpassen. Voor toewijzing van de gevorderde dwangsom bestaat gelet hierop geen aanleiding. Die

aanleiding ontbreekt hoe dan ook, omdat de Staat rechterlijke veroordelingen nakomt. Anders dan eisers stellen is het overigens volstrekt niet gebruikelijk dat aan veroordelingen van de Staat een dwangsom wordt verbonden.

7.3 De Staat gaat hierna ten overvloede afzonderlijk in op de formulering van de vorderingen, nu deze zeer algemeen en onbepaald van aard is en de nodige vragen oproept. Ook daarop stuit toewijzing af.

7.4 Voorop gesteld wordt dat ingeval van enige toewijzing vast moet staan dat in alle daardoor bestreken gevallen sprake moet zijn van onrechtmatig handelen. Dat is gezien de onbepaaldheid van de vorderingen al niet goed mogelijk. Bovendien zal enige toewijzing zo moeten worden geformuleerd dat duidelijk is wat als onrechtmatig handelen moet worden beschouwd en waarop een eventueel verbod dan zou zien. Ook dat is in het geval van de vorderingen zoals die in het petitum zijn geformuleerd niet het geval. De vorderingen zoals die in het petitum zijn geformuleerd worden gekenmerkt door een groot aantal en/of-formuleringen, waarvan onduidelijk is wat eisers daarmee voor ogen staat. Zo zou de rechtbank voor recht moeten verklaren (I) dat de Staat in strijd handelt met Nederlands recht (...) door van buitenlandse inlichtingen- en veiligheidsdiensten gegevens te ontvangen *of* te gebruiken en de Staat moeten verbieden (II) gegevens van buitenlandse inlichtingen- en veiligheidsdiensten te ontvangen *of* te gebruiken in strijd met Nederlands recht *of* gegevens waarvan niet met zekerheid is vast te stellen dat dit niet het geval is. Wat bedoelen eisers hiermee? En wie maakt hier de keus? De door eisers gekozen formulering zou, indien in deze vorm in een dictum overgenomen, in de praktijk tot vele uitvoeringsvragen en hernieuwde discussies aanleiding geven.

7.5 Belangrijker bezwaar is nog de algemene formulering van de vorderingen. Eisers vorderen immers dat de rechtbank (I) voor recht verklaart dat de Staat, kort gezegd, in strijd handelt met Nederlands recht door gegevens van buitenlandse inlichtingendiensten te ontvangen en te gebruiken die "via ongeoorloofde middelen" zijn vergaard, "zoals met behulp van PRISM of vergelijkbare programma's"; dat gebruik moet bovendien worden verboden. Er zal duidelijk omschreven moeten worden om welke "ongeoorloofde middelen" het precies gaat, hetgeen eisers hebben nagelaten. Verder zijn de stellingen in de dagvaarding toegespitst op de informatievergaring door de NSA, met toepassing van het programma PRISM. Een omschrijving van het programma PRISM ontbreekt evenwel, zodat onduidelijk is wat daarmee nu precies wordt bedoeld en waarin enigerlei onrechtmatigheid volgens eisers zou zijn gelegen. Dat staat eraan in de weg dat een verklaring voor recht zou worden uitgesproken ten aanzien van gegevens die zijn vergaard "met het programma PRISM", en a fortiori ten aanzien van gegevens die zijn vergaard met "vergelijkbare programma's". Dan kan in het midden blijven dat de NSA, overigens net zo min als andere buitenlandse inlichtingen- en veiligheidsdiensten, bij de verstrekking van gegevens geen mededelingen doet over de wijze waarop die gegevens zijn vergaard of

de bron waarvan ze afkomstig zijn, zodat dat bij de Staat niet bekend is. En zo de stellingen al tot toewijzing van enige vordering ten aanzien van het gebruik van gegevens van de NSA zouden kunnen leiden, hetgeen de Staat betwist, kunnen zij nog niet tot toewijzing van enige vordering ten aanzien van het gebruik van gegevens van (alle?) andere buitenlandse inlichtingen- en veiligheidsdiensten met wie de Staat samenwerkt leiden. De stellingen richten zich daar immers niet op.

7.6 In onderdeel III wordt gevorderd dat de Staat wordt gelast alle passende maatregelen te treffen om de persoonlijke levenssfeer en/of de vrijheid van nieuwsgaring van eisers te beschermen. In onderdeel 87 van de dagvaarding lichten eisers dit toe door te verwijzen naar artikelen 10, 11 en 12 van de Privacyrichtlijn (95/46/EG). Zij lichten dat verder niet toe, waarop toewijzing al moet afstuiten. Zij laten bovendien na in te gaan op het specifieke karakter van de gegevensverwerking waarover het hier gaat, nl. gegevensverwerking met het oog op de bescherming van de nationale veiligheid. Daarvoor geldt een apart regiem. Ook daarop moet toewijzing afstuiten.
Wat eisers bedoelen met "alle passende maatregelen" wordt uitgewerkt in drie subonderdelen. Het onderscheid tussen subonderdelen (i) en (ii) is niet duidelijk. En hoe stellen eisers zich de toetsing voor, in zijn algemeenheid en met name ook van de gegevens "waarvan niet met zekerheid is vast te stellen" dat zij niet in strijd met het Nederlands recht zijn verkregen? Verder is onduidelijk om welke personen het hier gaat, nu het bij de eisers sub 6 t/m 9 gaat om "degenen wier belangen zij ingevolge hun statuten behartigen". Kennelijk is dat, in elk geval voor eiseres sub 9, iedereen. Daarop moet toewijzing al afstuiten. Eisers gaan er bovendien aan voorbij dat in (art. 47 e.v. van) de WIV 2002 een kennisnemingsregeling is opgenomen. Tegen onwelgevallige besluiten op verzoeken om kennisneming staat bestuursrechtelijke rechtsbescherming open, hetgeen bemoeienis van de civiele rechter uitsluit. Zo al geen sprake zou zijn van niet-ontvankelijkheid van de eisers in vordering III, moet toewijzing van deze vordering hierop in elk geval afstuiten. Een notificatieverplichting zoals eisers die kennelijk op het oog hebben is er niet, zoals in deze conclusie van antwoord uitvoerig is toegelicht.

## 8 Bewijs

8.1 De bewijslast in deze zaak rust primair op eisers. Eisers hebben evenwel in de eerste plaats een juridisch vraagstuk aan de rechtbank voorgelegd, waarbij zich (getuigen)bewijs slecht laat denken. Niettemin biedt de Staat bewijs van zijn stellingen aan door middel van getuigen en door middel van schriftelijk bewijs. Daarbij doet zich evenwel een belangrijke beperking voor die verband houdt met de aard van de materie, die in het voorgaande uitvoerig is besproken. De AIVD en MIVD kunnen en mogen in het openbaar geen uitspraken doen over hun concrete, operationele activiteiten. De ministers van BZK en Defensie kunnen er in de Tweede Kamer ook geen informatie over geven, anders dan vertrouwelijk via de Commissie IVD. De AIVD en MIVD kunnen er in deze procedure evenmin uitspraken over doen. Dat zou in strijd

met de wet zijn. Zo wordt bijvoorbeeld in artikel 15 van de WIV 2002 het hoofd van de AIVD de zorgplicht opgelegd voor de geheimhouding van daarvoor in aanmerking komende gegevens, de daarvoor in aanmerking komende bronnen waaruit de gegevens afkomstig zijn en de veiligheid van de personen met wier medewerking gegevens worden verzameld. In artikel 85 is verder voor een ieder die betrokken is bij de wet een specifieke geheimhoudingsplicht opgenomen. Ook waar het gaat om de verstrekking van gegevens (zie met name de artikelen 38, 39 en 40) is – via verwijzing naar de artikelen 85 en 86 – voorzien in specifieke geheimhoudingsverplichtingen.

8.2 De WIV 2002 kent een gesloten verstrekkingenregiem, zodat gegevens alleen mogen worden verstrekt op de in de wet genoemde gronden en aan de in de wet genoemde ontvangers (zie expliciet art. 45). Dit stelsel legt beperkingen op aan de Staat als het gaat om bewijslevering waarmee rekening moet worden gehouden. De Staat is bereid om, indien de rechtbank dat voor de beoordeling van de vordering nodig zou achten en daarom, bijvoorbeeld met toepassing van artikel 22 Rv, zou verzoeken, geheime informatie vertrouwelijk, door analoge toepassing van artikel 8:29 Awb, aan de rechtbank ter kennis te brengen. De Staat wijst in dit verband op het arrest van de Hoge Raad van 11 juli 2008, ECLI:NL:HR:2008:BC8421, dat in deze mogelijkheid voorziet en daarvoor een procedure schetst. Voorop staat echter dat eisers algemene, niet geconcretiseerde stellingen innemen en dat van de Staat niet mag worden verwacht dat hij daarop concreet, met vertrouwelijke en operationele informatie, reageert.

## 9 Conclusie

De Staat concludeert:

(i) tot niet-ontvankelijkverklaring van eisers in hun vorderingen, althans tot afwijzing van het gevorderde;

(ii) met veroordeling van eisers in de kosten van het geding, zulks met bepaling dat over die proceskostenveroordeling de wettelijke rente verschuldigd zal zijn met ingang van de vijftiende dag na de datum van het te dezen te wijzen vonnis;

(iii) en met veroordeling van eisers in de nakosten, conform het liquidatietarief begroot op € 131 dan wel in het geval van betekening € 199;

(iv) met verklaring dat de proceskostenveroordeling uitvoerbaar bij voorraad is.

Advocaat

| | |
|---|---|
| behandeld door | E.J. Daalder en C.M. Bitter |
| correspondentie | Postbus 11756, 2502 AT Den Haag |
| telefoon | (070) 515 37 17 |
| fax | (070) 515 30 76 |
| e-mail | ej.daalder@pelsrijcken.nl |
| zaaknr | 10041444 |

## Inventaris

**Staat / Nooitgedagt c.s.**
**Nr. C/09/455237, 2013/1325**

| | |
|---|---|
| 1 | *Kamerstukken II* 2012/2013, 30 977, nr. 56, met bijlage; |
| 2 | Council of the European Union, Report on the findings by the EU Co-chairs and the ad hoc EU-US Working Group on Data Protection, 27 November 2013, 16987/13; |
| 3 | *Kamerstukken II* 2012/2013, 30 977, nr. 59; |
| 4 | Brief Voorzitter van de Tweede Kamer van 16 juli 2013; |
| 5 | Brief CTIVD van 5 augustus 2013; |
| 6 | *Kamerstukken II* 2013/2014, 30 977, nr. 76; |
| 7 | *Kamerstukken II* 2013/2014, 30 977, nr. 63; |
| 8 | *Kamerstukken II* 2013/2014, 30 977, nr. 64; |
| 9 | *Kamerstukken II* 2013/2014, 30 977, nr. 75, p. 23-25; |
| 10 | *Kamerstukken II* 2013/2014, 30 977, nr. 65; |
| 11 | *Kamerstukken II* 2013/2014, 30 977, nr. 75, p. 18; |
| 12 | *Kamerstukken II* 2013/2014, 30 977, nr. 74; |
| 13 | *Kamerstukken II* 2013/2014, 30 977, nr. 75, p. 22; |
| 14 | Toezichtsrapport CTIVD nr. 28; |
| 15 | Toezichtsrapport CTIVD nr. 31; |
| 16 | Toezichtsrapport CTIVD nr. 35; |
| 17 | Toezichtsrapport CTIVD nr. 22A; |
| 18 | Clapper v. Amnesty International USA et al, 133 S.Ct. 1138 (2013); |
| 19 | *Klayman et al. v. Obama,* no. 13-0851 (D.D.C. 2013); |
| 20 | American Civil Liberties Union et al. v. James R. Clapper et al., no. 13-Civ, 3994 (WHP) (S.D.N.Y. 2013). |