bB

Gerechtshof Den Haag
Zitting van 2 februari 2016 om 10:00 uur
Zaaknummer 200.162.969/01

MEMORIE VAN GRIEVEN

in de zaak tussen

De heer **Bart Theophilus Nooitgedagt e.a.**,

Eisers,

Advocaten: mr. Chr. A. Alberdingk Thijm en mr. C.F.M. de Vries

en

De **Staat der Nederlanden (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)**,

Gedaagde,

Advocaat: mr. C.M. Bitter

bB

INHOUDSOPGAVE

INLEIDING

1. De Nederlandse inlichtingen- en veiligheidsdiensten, de AIVD en MIVD, werken samen met buitenlandse zusterdiensten, waaronder de Amerikaanse NSA en de Britse GCHQ. Met deze buitenlandse diensten, wisselen onze diensten grote hoeveelheden persoonsgegevens uit. Hoe nauwer de samenwerking, hoe groter de ruilhandel, want de gegevensuitwisseling is gebaseerd op het beginsel "quid pro quo".

2. In november 2013 werd bekend dat Nederland deel uitmaakt van de zogenaamde "Nine Eyes", een selecte groep van negen bondgenoten, die intensief samenwerken, waaronder de Verenigde Staten en Groot-Brittannië. Daarmee staat Nederland slechts één trede lager dan de vier landen waarmee de Amerikanen het nauwst samenwerken, de zogenaamde "Five Eyes" (de Verenigde Staten, Groot-Brittannië, Canada, Australië en Nieuw-Zeeland).

3. De samenwerking met de Britten en Amerikanen is er een gebaseerd op "vertrouwen". De AIVD en MIVD vertrouwen erop dat de buitenlandse diensten mensenrechten respecteren en handelen binnen de eigen nationale regelgeving.[1]

4. De vraag die in deze zaak voorligt is of de Staat die samenwerking op dezelfde manier mag vervolgen. Mag de Staat de samenwerking op basis van "vertrouwen" voortzetten na alle Snowden-onthullingen, die hebben aangetoond op wat voor schaal de Amerikanen en Britten inbreuk plegen op de persoonlijke levenssfeer van burgers. Snowden heeft aangetoond dat de NSA en GCHQ geen middel ongemoeid laten om ongelimiteerd toegang te kunnen krijgen tot de (persoons)gegevens van alles en iedereen. De juistheid van een groot deel van de onthullingen van Snowden wordt niet betwist.[2] Mogen de Nederlandse diensten in de samenwerking met onder meer de NSA en GCHQ de ogen sluiten voor de permanente inbreuken op de persoonlijke levenssfeer die deze diensten verrichten?

5. Eisers menen van niet. Via buitenlandse diensten krijgen de AIVD en de MIVD immers de beschikking over gegevens die met ongeoorloofde middelen zijn verkregen, onder meer met gebruikmaking van PRISM, Upsteam, TEMPORA of een van de andere talloze programma's van de NSA en GCHQ. Door te blijven samenwerken zonder dat de MIVD en AIVD zich vergewissen van de herkomst van de gegevens die zij op grond van deze samenwerking verkrijgen, komt dit neer op het "witwassen" van illegale data. De Staat krijgt toegang tot gegevens die zij zelf nooit had mogen vergaren.

6. Eisers zijn er in deze zaak niet op uit om de samenwerking met buitenlandse diensten als zodanig uit te bannen. Maar zij menen wel dat er bij het samenwerken en bij het uitwisselen van gegevens, waarborgen in acht moeten worden genomen. Waarborgen die alom zijn geaccepteerd en voortvloeien uit de jurisprudentie van onder meer het EHRM. Het gaat eisers om de grenzen van de samenwerking. Nederlandse diensten moeten geen gebruik (willen) maken van informatie die is verkregen door de inzet van illegale methodes.

[1] Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD, 5 februari 2014, CTIVD nr. 38, p. xi.
[2] Conclusie van Advocaat-Generaal Y. Bot van 23 september 2015, Zaak C 362/14 (*Schrems*), ov. 36.

7. Eerder, in december 2013, adviseerde de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (hierna: "CTIVD") al de samenwerking met de VS te herzien. De Snowden-onthullingen maken dat het gewenst is om na te gaan of het "vertrouwen" in de zusterorganisaties nog steeds gewenst is, zo concludeerde de CTIVD. Bovendien moeten onze diensten zich onthouden van het gebruik van gegevens waarvan bekend is of vermoed wordt dat zij door de buitenlandse dienst zijn verworven met gebruik van een methode die een ongeoorloofde inbreuk op een grondrecht vormt (**productie 8, p. 31-32**). Ook de Commissie Dessens, die de Wiv evalueerde, vindt dat het wettelijk kader inzake de samenwerking heroverweging verdient en dat, mede in het licht van de NSA-onthullingen, nader onderzocht moet worden of de Wiv voor de samenwerking met buitenlandse diensten voldoende rechtsstatelijke en democratische garanties bevat (**productie 11**).

8. De rechtbank heeft in haar vonnis van 23 juli 2014 echter geoordeeld dat de samenwerking op basis van vertrouwen tussen onze diensten en de Amerikanen en andere diensten, gewoon mag worden voortgezet. Het zwaarwegende belang van de nationale veiligheid geeft voor dit oordeel de doorslag (r.o.5.38). Daarmee heeft de rechtbank de diensten carte blanche gegeven, louter vanwege het predicaat "nationale veiligheid". Omdat er geen deugdelijk toezicht is op de diensten, is enkel hun woord voldoende om inbreuken op de persoonlijke levenssfeer te legitimeren. Wanneer gegevensuitwisseling voorzien worden van het stempel "nationale veiligheid" moet de rechtsstaat wijken, althans zo lezen eisers de beslissing van de rechtbank.

9. De rechtbank neemt als uitgangspunt dat het bij de uitwisseling van gegevens tussen inlichtingendiensten enkel gaat om de uitwisseling van "ruwe" data in bulk. Nog los van de vraag of dit juist is, heeft de rechtbank miskend dat de uitwisseling van bulk-data zelfs nog kwalijker is dat de uitwisseling van specifieke informatie, omdat bulkdata ook veel onschuldige mensen betreft.

10. De rechtbank vindt verder dat het recht op privacy minder gewicht in de schaal legt bij internationale samenwerking tussen inlichtingendiensten. Volgens de rechtbank moet in die situatie het voorzienbaarheidsvereiste minder stringent moet worden toegepast en zijn minder verstrekkende waarborgen vereist (r.o. 5.29). Dit oordeel vindt geen steun in het recht. Integendeel, uit de rechtspraak van het EHRM volgt juist dat omdat de werkwijze van geheime diensten zich onttrekt aan de democratische controle, die werkwijze een voldoende duidelijke wettelijke basis moet hebben. Waarborgen zijn daarom met name bij geheime bevoegdheden essentieel.

11. De rechtbank overweegt verder dat het uit het oogpunt van de nationale veiligheid niet van de Staat kan worden verwacht dat hij de samenwerking met buitenlandse diensten verbreekt (r.o. 5.34). De staande praktijk, waarbij de diensten elkaar niet plegen te informeren over hun bronnen, hoeft niet te worden doorbroken. Kennelijk biedt de *modus operandi* de Staat dus wel degelijk een vrijbrief.

12. De rechtbank heeft ten slotte geoordeeld dat niet aan de orde is de vraag of het noodzakelijk is om gegevens te verkrijgen die in strijd met artikel 8 EVRM zijn verkregen, maar dat het gaat om

de “dringende maatschappelijke” behoefte dat met buitenlandse diensten wordt samengewerkt. Door aldus te redeneren keert de rechtbank het noodzakelijkheidsvereiste om.

13. Eisers kunnen zich met het vonnis niet verenigen en voeren daartegen 14 grieven aan. Het oordeel van de rechtbank is onjuist en niet (langer) houdbaar. De samenwerking met de Amerikanen en Britten kan niet op dezelfde voet worden voorgezet, zeker niet in het licht van recente ontwikkelingen.

14. Het Europese Hof van Justitie heeft inmiddels geoordeeld. Het uitwisselen van gegevens met de Amerikanen is volgens het HvJEU enkel geoorloofd als de Amerikanen een niveau van bescherming van grondrechten bieden dat in grote lijnen overeenstemt met het recht van de Unie. Het HvJEU oordeelt dat de Verenigde Staten deze drempel niet halen. Wat de Amerikanen doen, gaat simpelweg veel te ver. Het HvJEU benadrukt in dit kader het belang van waarborgen, ook – juist – als het gaat om automatische verwerking van bulkgegevens. De uitspraak in *Schrems* maakt duidelijk dat de gegevensuitwisseling met de Amerikanen met waarborgen moet worden omkleed, wil deze geoorloofd zijn. Zou dat anders zijn, dan zouden de strenge, Europese privacy regels, op eenvoudige wijze kunnen worden omzeild.[3]

15. Het Hof Den Haag oordeelde intussen dat de Wiv onvoldoende waarborgen biedt ter bescherming van het fundamentele verschoningsrecht van advocaten en aarzelde terecht niet om de Staat een positieve verplichting op te leggen.[4]

16. De regering vindt overig kennelijk zelf ook dat de huidige Wiv niet aan artikel 8 EVRM voldoet, want kondigde in 2015 een integrale wijziging van de wet aan.[5] De bepaling over internationale samenwerking wordt ook aangepast, al vindt de CTIVD nog steeds dat deze niet voldoet.

17. De grieven, in onderling verband beschouwd, beogen het geschil in volle omvang ter beoordeling aan uw Hof voor te leggen. Eisers handhaven uitdrukkelijk alle stellingen die zij in eerste aanleg hebben aangevoerd. Volledigheidshalve zij opgemerkt dat dit ook geldt voor de zijdens eisers gestelde gronden, feiten en omstandigheden welke niet of onvolledig zijn weergegeven in het vonnis waarvan beroep. Eisers blijven verder de stellingen en standpunten van de Staat betwisten, een en ander voor zover deze niet nadrukkelijk in prima zijn of in appel worden erkend.

18. Hieronder zal eerst worden ingegaan op het recente ontwikkelingen, waarna eisers hun grieven zullen toelichten.

---

[3] HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*).
[4] Hof Den Haag 27 oktober 2015, ECLI:NL:GHDHA:2015:2881. Bekrachtiging van Rb. Den Haag 1 juli 2015, ECLI:NL:RBDHA:2015:7436.
[5] Concept-wetsvoorstel Wet op de Inlichtingen- en veiligheidsdiensten 20XX (consultatieversie juni 2015), te vinden op: https://www.internetconsultatie.nl/wiv.

ONTWIKKELINGEN SINDS HET VONNIS

19. Sinds het vonnis in eerste aanleg hebben zich een aantal belangrijke ontwikkelingen voorgedaan die van belang zijn voor de beoordeling van het onderhavige hoger beroep. Die ontwikkelingen zullen hieronder kort worden besproken.

Wijziging Wiv

20. In juli 2015 kondigt het kabinet een ingrijpende wijziging van de Wet op inlichtingen- en veiligheidsdiensten ("Wiv") aan. De Wiv 2002 wordt integraal vervangen door een nieuwe wet. Aanleiding daartoe vormt de in 2013 uitgevoerde evaluatie van de Wiv 2002 door de commissie Dessens (**productie 11**).[6]

21. Deze Commissie Dessens had in haar evaluatie van de Wiv onder meer overwogen dat "*het wettelijk kader in artikel 59 heroverweging verdient en dat, mede in het licht van de recente discussies over de NSA, nader onderzocht moet worden of de Wiv voor de samenwerking met buitenlandse diensten voldoende rechtsstatelijke en democratische garanties bevat*." (**productie 11, p. 119**). Het kabinet heeft in reactie op dit rapport aangegeven dat zij het eens is met de conclusie van de Commissie Dessens (**productie 12, p. 6**).

22. Ook de CTIVD had de ministers in haar laatste toezichtrapport (rapport 38, **productie 8**) geadviseerd de samenwerking te herzien.

> *De Commissie constateert dat de AIVD en de MIVD in de onderzochte hechte samenwerkingsverbanden er in grote mate op vertrouwen dat de desbetreffende buitenlandse diensten mensenrechten respecteren en handelen binnen de eigen nationale regelgeving. De Commissie is van mening dat het in het licht van de onthullingen van de afgelopen periode gewenst is om na te gaan of dit vertrouwen nog steeds terecht is […] De Commissie beveelt de ministers van BZK en van Defensie in dit verband tevens aan de samenwerkingsrelaties (ook in internationaal verband) te beoordelen op transparantie en de afwegingen die ten grondslag liggen aan de samenwerking nader te concretiseren.* (**productie 8, p. 31**).

23. Dat gebeurt ook. Het bestaande kader is aan heroverweging en verdere uitbouw toe, zo stelt de regering in de Memorie van Toelichting. "Zowel de rapporten van de CTIVD als de aanbevelingen van de commissie Dessens ter zake, alsmede hetgeen met in het bijzonder de Tweede Kamer in dit verband is gewisseld, nopen daartoe".[7] Daarmee erkent het kabinet dat het huidige artikel 59 op dit moment niet voldoet en niet voorziet in voldoende waarborgen.

24. Een en ander heeft in het wetsvoorstel geresulteerd in een nieuw artikel 76, dat gaat over de samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten. Artikel 76 van het wetsvoorstel luidt:

---

[6] Rapport Commissie Dessens, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, 2 december 2013.
[7] Memorie van Toelichting bij het concept-wetsvoorstel Wet op de Inlichtingen- en veiligheidsdiensten 20XX (consultatieversie juni 2015), p. 136.

1. *De diensten zijn bevoegd tot het aangaan van samenwerkingsrelaties met daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen.*
2. *Voorafgaand aan het aangaan van een samenwerkingsrelatie als bedoeld in het eerste lid weegt de dienst aan de hand van de criteria als bedoeld in het derde lid of kan worden overgegaan tot het aangaan van een samenwerkingsrelatie en, zo ja, wat de aard en intensiteit van de beoogde samenwerking kan zijn.*
3. *Bij de weging als bedoeld in het tweede lid worden in ieder geval de volgende criteria betrokken:*
    a. *de democratische inbedding van de dienst in het desbetreffende land;*
    b. *de eerbiediging van de mensenrechten door het desbetreffende land;*
    c. *de professionaliteit en betrouwbaarheid van de desbetreffende dienst.*
4. *Een samenwerkingsrelatie met een inlichtingen- en veiligheidsdienst van een ander land wordt pas aangegaan, indien daartoe door Onze betrokken Minister toestemming is verleend. Onze betrokken Minister kan de bevoegdheid tot het verlenen van toestemming mandateren aan het hoofd van de dienst. Van een verleende toestemming door het hoofd van de dienst wordt Onze betrokken Minister zo spoedig mogelijk geïnformeerd.*
5. *Het hoofd van de dienst draagt er zorg voor dat indien omstandigheden daartoe aanleiding geven de aard en intensiteit van de samenwerkingsrelatie met een inlichtingen- en veiligheidsdienst van een ander land opnieuw wordt gewogen. Het tweede tot en met vierde lid is van overeenkomstige toepassing.*

25. Het artikel geeft enkel een regeling ten behoeve van het *aangaan* van samenwerkingsrelaties en de aard en intensiviteit daarvan.[8] De Commissie Dessens en de CTIVD zijn in zoverre gevolgd dat de criteria om te beoordelen met welke diensten wordt samengewerkt en tot op welk niveau nu met zoveel woorden zijn opgenomen in het concept artikel.

26. Rechtsstatelijke en democratische garanties over de *inhoud* van die samenwerking, eveneens aanbevolen door de Commissie Dessens (**productie 12, p. 119**), ontbreken echter. Evenmin bevat het conceptartikel een bepaling die specifiek ziet op de bevoegdheid tot het *ontvangen* en *gebruiken* van gegevens afkomstig van buitenlandse diensten door de Nederlandse diensten.

27. De memorie van toelichting vermeldt wel dat bij de weging die moet worden verricht voorafgaand aan de samenwerking, ook de risico's die aan de eventuele samenwerking verbonden zijn in kaart moeten worden gebracht. Daarbij moet volgens de toelichting onder meer worden gedacht aan "zaken als ten aanzien van welke onderwerpen onder welke omstandigheden gegevensuitwisseling kan plaatsvinden en aan welke andere voorwaarden moet worden voldaan". "Het uitwisselen van persoonsgegevens verdient hierbij uitdrukkelijk de aandacht", aldus de toelichting.[9]

[8] Memorie van Toelichting bij het concept-wetsvoorstel Wet op de Inlichtingen- en veiligheidsdiensten 20XX (consultatieversie juni 2015), p. 140.
[9] Memorie van Toelichting bij het concept-wetsvoorstel Wet op de Inlichtingen- en veiligheidsdiensten 20XX (consultatieversie juni 2015), p. 139.

28. Aan wat voor voorwaarden en omstandigheden voor gegevensuitwisseling moet worden gedacht, vermeldt de toelichting echter niet. Inhoudelijke criteria over die uitwisseling van gegevens ontbreken volledig.

Reactie CTIVD

29. De CTIVD heeft in augustus 2015 gereageerd op het in consultatie gegeven wetsvoorstel, dat in totaal 557 – doorgaans kritische – reacties heeft uitgelokt.

30. Ook de toezichthouder is kritisch ten aanzien van het wetsvoorstel en de daarin vervatte waarborgen. Het voornaamste gebrek is volgens de CTIVD dat zij als toezichthouder geen bindend rechtmatigheidsoordeel toekomt, terwijl effectief toezicht vereist dat een onafhankelijke toezichthouder de bevoegdheid heeft om bij onrechtmatig optreden in te grijpen. De toezichthouder mist "tanden", aldus de CTIVD.[10] De CTIVD acht het onder meer van essentieel belang dat op de ministeriële lastgeving achteraf bindend toezicht kan worden uitgeoefend.[11]

31. De CTIVD verwijst in dit verband naar de bijlage bij haar reactie, bestaande uit een uitgebreide studie van de Universiteit Leiden, "Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten". In dit rapport wordt in kaart gebracht welke minimumeisen en verdere richtinggevende voorwaarden uit de EHRM-jurisprudentie en andere mensenrechteninstanties voortvloeien met betrekking tot de inrichting en vormgeving van het toezicht op de inlichtingen- en veiligheidsdiensten. Geconcludeerd wordt dat het EHRM weliswaar een sterke voorkeur heeft voor *ex ante* toestemmingsverlening door een onafhankelijke autoriteit voor de inzet van heimelijke onderzoeksbevoegdheden, maar dat in ieder geval dient te worden voorzien in een bindend *ex post* rechtmatigheidstoezicht door een externe onafhankelijke toezichthouder. De ontwikkeling in het internationale en Europese privacydebat en het feit dat de ongerichte communicatie-interceptie naar zijn aard een grootschalig karakter heeft, waardoor in potentie heel veel burgers en communicatiestromen kunnen worden geraakt, dwingt Nederland ertoe ten minste te voorzien in de mogelijkheid van bindende rechtmatigheidsoordelen van de CTIVD, zo concluderen de onderzoekers.[12]

32. De CTIVD is ook kritisch over de voorgestelde bevoegdheid tot grootschalige interceptie (bulk) dat het wetsvoorstel bevat (artikel 33 e.v.). Volgens de toezichthouder ontbreken adequate waarborgen tegen ongeoorloofde inbreuken. Onder meer de voorgestelde bewaartermijnen – één jaar voor gericht verzamelde gegevens en drie jaar voor bulkgegevens – zijn naar de mening van de CTIVD te lang. De CTIVD verwijst in dit verband nadrukkelijk naar de Digital Rights-uitspraak van het HvJEU.[13]

33. De CTIVD plaatst verder kanttekeningen bij de voorgestelde bepalingen die zien op de samenwerking met buitenlandse diensten en dan met name op het verstrekken van gegevens

[10] Reactie CTIVD op het concept-wetsvoorstel wet op inlichtingen- en veiligheidsdiensten 20XX, 26 augustus 2015, p. 11.
[11] Reactie CTIVD op het concept-wetsvoorstel wet op inlichtingen- en veiligheidsdiensten 20XX, 26 augustus 2015, p. 11, p. 14-15.
[12] Mr. dr. J.P. Loof, mr. dr. J. Uzman, prof. mr. T. Barkhuysen, prof. mr. A.C. Buyse, prof. mr. J.H. Gerards, prof. dr. R.A. Lawson, *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, augustus 2015, p. II-II.
[13] Reactie CTIVD op het concept-wetsvoorstel wet op inlichtingen- en veiligheidsdiensten 20XX, 26 augustus 2015, p. 46-47.

aan buitenlandse diensten. De CTIVD acht het van belang dat zoveel mogelijk zicht wordt verkregen op de manier waarop door een ontvangende buitenlandse dienst omgegaan zal worden met niet geëvalueerde gegevens. Bij de beoordeling van de samenwerkingscriteria moet volgens de CTIVD expliciet aandacht worden besteed aan de waarborgen op het gebied van gegevensverwerking, opslag van gegevens en vernietiging van de gegevens bij de ontvangende dienst.[14] Bovendien zijn volgens de CTIVD aanvullende waarborgen op zijn plaats waar het de verstrekking van persoonsgegevens aan buitenlandse diensten betreft. Zo acht de CTIVD de waarborg van ministeriële toestemming in plaats van interne toestemming op zijn plaats. Anders ziet de CTIVD niet in hoe Nederland kan voldoen aan zijn mensenrechtelijke verplichtingen.[15]

Schrems

34. Op 6 oktober 2015 heeft het HvJEU in de zaak *Schrems* een baanbrekende uitspraak gedaan over de uitwisseling van gegevens met de Verenigde Staten. Kort gezegd, oordeelt het HvJEU dat de VS geen "passend beschermingsniveau" bieden vanwege de handelwijze van de NSA.

35. In de Schrems-uitspraak vernietigt het HvJEU om die reden de beschikking van de Europese Commissie op grond waarvan een passende beschermingsniveau voor de doorgifte van gegevens naar de VS werd bereikt indien organisaties voldeden aan de zogenaamde "Safe Harbor" beginselen.

36. De Snowden-onthullingen vormden de aanleiding voor de procedure.

> *Een aantal onthullingen heeft recent immers het bestaan van Amerikaanse programma's aan het licht gebracht waarmee op grote schaal informatie wordt verzameld. Deze onthullingen hebben bezorgdheid gewekt over de eerbiediging van de normen van Unierecht bij de doorgifte van persoonsgegevens naar in de Verenigde Staten gevestigde ondernemingen en over de zwakke punten van de veiligehavenregeling.*[16]

37. In zijn arrest verduidelijkt het HvJEU wat onder een "passend beschermingsniveau" moet worden verstaan. Daarvan is sprake als het land een niveau van bescherming biedt van grondrechten dat in grote lijnen overeenstemt met de Europese normen.

> *[D]e uitdrukking „passend beschermingsniveau" [moet] zo worden opgevat dat die vereist dat het derde land, op grond van zijn nationale wetgeving of zijn internationale verbintenissen, een niveau van bescherming van de grondrechten en de fundamentele vrijheden biedt dat in grote lijnen overeenkomt met het niveau dat binnen de Unie wordt gewaarborgd.*[17]

[14] Reactie CTIVD op het concept-wetsvoorstel wet op inlichtingen- en veiligheidsdiensten 20XX, 26 augustus 2015, p. 52-53.
[15] Reactie CTIVD op het concept-wetsvoorstel wet op inlichtingen- en veiligheidsdiensten 20XX, 26 augustus 2015, p. 54.
[16] Conclusie van Advocaat-Generaal Y. Bot van 23 september 2015, Zaak C 362/14 (*Schrems*), ov. 4.
[17] HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*), r.o. 73.

38. Het HvJEU verduidelijkt ook waarom alleen gegevens mogen worden doorgegeven aan landen die een dergelijk passend beschermingsniveau bieden. Zou dat anders zijn, dan zouden de strenge, Europese privacyregels, op eenvoudige wijze kunnen worden omzeild.

> *Indien een dergelijk vereiste* [van een passend beschermingsniveau, advocaat] *zou ontbreken, zou dat immers in strijd zijn met de in het vorige punt genoemde doelstelling* [om het hoge niveau van bescherming te continueren bij doorgifte van gegevens naar derde landen]. *Bovendien zou het hoge beschermingsniveau dat bij richtlijn 95/46, gelezen in samenhang met het Handvest, wordt gewaarborgd, eenvoudig kunnen worden omzeild door persoonsgegevens vanuit de Unie naar derde landen door te geven teneinde in die landen te worden verwerkt.*[18]

39. Hoewel de waarborgen die in het derde land een passend beschermingsniveau moeten garanderen, kunnen verschillen van die welke binnen de Unie gelden, moeten deze waarborgen in de praktijk wel doeltreffend genoeg zijn om een bescherming te bieden die in grote lijnen overeenkomt met die welke binnen de Unie wordt gewaarborgd.[19]

40. Het HvJEU oordeelt dat dergelijke doeltreffende waarborgen in de VS ontbreken. De eisen van de nationale veiligheid in de VS hebben namelijk altijd voorrang boven de Safe Harbors. Amerikaanse organisaties die zich hebben aangesloten bij de Safe Harbor beginselen zijn verplicht om zonder beperking van die beginselen af te wijken, wanneer die beginselen conflicteren zijn met de Amerikaanse regelgeving op het gebied van nationale veiligheid.[20] De Snowden-onthullingen hebben immers laten zien dat de Amerikaanse autoriteiten zich op grote schaal en ongedifferentieerd toegang kunnen verschaffen tot persoonsgegevens van de bevolking van de Unie.[21] A-G Bot schrijft hierover:

> *Enerzijds kunnen persoonsgegevens die door ondernemingen als Facebook Ireland aan hun in de Verenigde Staten gevestigde moedervennootschap zijn doorgegeven vervolgens worden geraadpleegd door de NSA en andere Amerikaanse veiligheidsdiensten tijdens grootschalige en niet-gerichte surveillance- en onderscheppingsactiviteiten. Na de onthullingen van Snowden kan thans immers geen enkele andere plausibele conclusie worden getrokken uit het beschikbare bewijsmateriaal. Anderzijds beschikken de burgers van de Unie over geen enkel effectief recht om te worden gehoord over het surveilleren en onderscheppen van hun gegevens door de NSA en andere Amerikaanse veiligheidsdiensten.*
> *[…]*
> *Deze feiten tonen mijns inziens aan dat beschikking 2000/520 onvoldoende waarborgen bevat.*[22]

41. Een dergelijk, algemeen, primaat van de Amerikaanse wetgeving op het gebied van nationale veiligheid is volgens het HvJEU ontoelaatbaar, want brengt het risico met zich mee dat het

[18] HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*), r.o. 73.
[19] HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*), r.o. 74.
[20] HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*), r.o. 86.
[21] Conclusie van Advocaat-Generaal Y. Bot van 23 september 2015, Zaak C 362/14 (*Schrems*), ov. 4.
[22] Conclusie van Advocaat-Generaal Y. Bot van 23 september 2015, Zaak C 362/14 (*Schrems*), ov. 155, 159.

recht op privacy van Europese burgers wordt beperkt. Daarbij is het volgens het HvJEU van weinig belang of de gegevens al dan niet gevoelig zijn en of de betrokkenen door die inmenging enig nadeel ondervinden.[23]

42. Het HvJEU, onder verwijzing naar zijn eerdere uitspraak in *Digital Rights Ierland* en de rechtspraak van het EHRM, onderstreept het belang van duidelijke en precieze regels en waarborgen wanneer een bevoegdheid een inmenging van het recht op privacy met zich meebrengt. De noodzaak daarvan is volgens het HvJEU des te groter wanneer de persoonsgegevens automatisch worden verwerkt en er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd.

> *Wat het binnen de Unie gewaarborgde niveau van bescherming van de grondrechten en fundamentele vrijheden betreft, moet een regeling van de Unie die een inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten met zich brengt, volgens vaste rechtspraak van het Hof duidelijke en precieze regels betreffende de draagwijdte en de toepassing van een maatregel bevatten en minimale vereisten opleggen, zodat de personen van wie de persoonsgegevens aan de orde zijn, over voldoende garanties beschikken dat hun gegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens. De noodzaak om over dergelijke garanties te beschikken is des te groter wanneer de persoonsgegevens automatisch worden verwerkt en er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd (arrest Digital Rights Ireland e.a., C 293/12 en C 594/12, EU:C:2014:238, punten 54 en 55 en aldaar aangehaalde rechtspraak).*

43. Beperkingen van het recht op privacy moeten verder, willen zij geoorloofd zijn, binnen de grenzen van het strikt noodzakelijke blijven. De Amerikaanse praktijk voldoet niet aan die eis. Op grond daarvan mogen de Amerikaanse diensten immers in zijn algemeenheid persoonsgegevens van alle personen bewaren, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het nagestreefde doel.[24]

44. Het HvJEU specificeert verder dat een regeling, op grond waarvan de Amerikaanse autoriteten in zijn algemeenheid toegang kunnen krijgen tot de inhoud van communicatie, moet worden beschouwd als een aantasting van de wezenlijke inhoud van het grondrecht op eerbiediging van het privéleven.[25]

45. De uitspraak van het HvJEU is om meerdere redenen van groot belang voor de onderhavige zaak:

- Het HvJEU maakt duidelijk dat derde landen waarmee gegevens worden uitgewisseld daadwerkelijke waarborgen moeten bieden voor een niveau van bescherming van de

[23] HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*), r.o. 87.
[24] HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*), r.o. 93.
[25] HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*), r.o. 94.

grondrechten dat in grote lijnen overeenkomt met het niveau van bescherming in Europa;
- Het HvJEU maakt eveneens duidelijk dat de Amerikaanse wetgeving en de algemene, verstrekkende bevoegdheden van de Amerikaanse geheime diensten om (bulk)data te verzamelen, niet aan die eis voldoen;
- Het HvJEU benadrukt dat de gegevensuitwisseling met landen die geen passend beschermingsniveau bieden, resulteert in een omzeiling van het beschermingsniveau in Europa;
- Het HvJEU benadrukt – net als het EHRM – het belang van waarborgen, zeker als het automatische gegevensverwerkingen in bulk betreft, teneinde inmengingen in het recht op privacy zo beperkt mogelijk te houden.

46. Ook is deze zaak is sprake van omzeiling van de Europese privacywaarborgen. De Nederlandse diensten omzeilen het recht op privacy door gebruik te maken van gegevens die de buitenlandse diensten hebben verstrekt, zonder dat deze gegevens zijn verzameld met inachtneming van de persoonlijke levenssfeer van Nederlandse burgers.

47. Bovendien geldt dat de organisaties die voorheen gebruik maakten van de Safe Harbor-regeling om gegevens door te geven naar Amerika – bijvoorbeeld Facebook, Google, Microsoft, Apple en Yahoo[26] – allemaal betrokken zijn bij het PRISM-programma. Dat concludeert ook de Europese Commissie in 2013:

> *In de loop van 2013 heeft informatie over de schaal en de omvang van Amerikaanse observatieprogramma's vragen doen rijzen over de continuïteit van de bescherming van persoonsgegevens die rechtmatig aan de VS zijn doorgegeven in het kader van de veilige havenregeling. Alle ondernemingen die betrokken zijn bij het PRISM-programma en die de autoriteiten van de VS toegang verlenen tot in de VS opgeslagen en verwerkte gegevens, lijken bijvoorbeeld gecertificeerd te zijn in het kader van de veilige haven. Dit heeft van de veilige haven een van de kanalen gemaakt waarlangs de Amerikaanse inlichtingendiensten toegang hadden tot Persoonsgegevens die oorspronkelijk in de EU waren verwerkt.*[27]

48. De inlichtingendiensten van onder meer de VS hebben op grond van hun bevoegdheden rechtstreeks en grootschalige toegang tot de gegevens die deze bedrijven verwerken. Het betreft onder meer gegevens van miljoenen Nederlandse en Europese burgers. Diezelfde gegevens, die door de Amerikanen op ongeoorloofde wijze worden verkregen, worden in het kader van de internationale samenwerking vervolgens weer teruggegeven aan Europese diensten. Dit resulteert eveneens in een omzeiling van de Europese normen.

[26] Mededeling van de Commissie aan het Europees Parlement en de Raad betreffende de werking van de veiligehavenregeling ("Safe Harbour") uit het oogpuntvan EU-burgers en in de EU gevestigde ondernemingen, Brussel 27 november 2013, Mededeling COM(2013) 847 final, p. 20.
[27] Mededeling van de Commissie aan het Europees Parlement en de Raad betreffende de werking van de veiligehavenregeling ("Safe Harbour") uit het oogpuntvan EU-burgers en in de EU gevestigde ondernemingen, Brussel 27 november 2013, Mededeling COM(2013) 847 final, p. 18.

Afluisteren advocaten onrechtmatig

49. Een andere relevante ontwikkeling betreft de uitspraken van de rechtbank respectievelijk het Hof Den Haag over het afluisteren van advocaten door de AIVD. Ook die uitspraken bevestigen dat de Wiv onvoldoende waarborgen ter bescherming van het recht op privacy bevat.

50. Advocatenkantoor Prakken d'Oliveira spant in juli 2015 een kort geding aan tegen de Staat, nadat is gebleken dat de AIVD communicatie van en met advocaten afluistert. Het advocatenkantoor eist in kort geding dat de AIVD daarmee stopt. Zij betogen dat advocaten en cliënten in vertrouwen met elkaar moeten kunnen communiceren. Het verschoningsrecht van advocaten vormt een ankerpunt van de rechtsstaat.

51. De rechtbank Den Haag oordeelt op 1 juli 2015 dat het onrechtmatig is om de communicatie van en met advocaten te tappen zonder onafhankelijke controle. De huidige bevoegdheid in de Wiv, op basis waarvan de minister voorafgaand toestemming moet geven, bevat onvoldoende waarborgen en voldoet daarmee niet aan de rechtspraak van het EHRM.[28] Het Hof Den Haag bekrachtigt dit vonnis op 27 oktober 2015.[29]

52. Zowel rechtbank als hof oordelen dat er onder de Wiv geen onafhankelijk orgaan is dat voorziet in onafhankelijk toezicht. De betrokken ministers zijn nu eenmaal niet onafhankelijk van de veiligheidsdiensten en de CTIVD toetst pas achteraf.

> *Vaststaat dat er onder de Wiv 2002 geen onafhankelijk orgaan is dat is voorzien met voormelde bevoegdheid. Naar het oordeel van de voorzieningenrechter biedt het bestaande systeem onvoldoende gelijkwaardige waarborgen. Weliswaar bestaat er […] beleid op grond waarvan voorafgaand aan het toepassen van bijzondere bevoegdheden jegens advocaten een verzwaarde proportionaliteitstoets plaatsvindt, maar de betrokken ministers zijn nu eenmaal niet onafhankelijk van de veiligheidsdiensten en de CTIVD toetst pas achteraf, zodat zij niet de mogelijkheid heeft om de uitoefening van bijzondere bevoegdheden jegens advocaten tegen te gaan of te beëindigen.*[30]
>
> *Het voorgaande betekent dat de voorzieningenrechter terecht tot het oordeel is gekomen dat direct en indirect tappen van advocaten slechts toelaatbaar is indien in onafhankelijk toezicht als hiervoor bedoeld is voorzien. Hij heeft ook terecht overwogen dat dergelijk onafhankelijk toezicht thans ontbreekt. Dat is tussen partijen overigens ook niet in geschil. De CTIVD heeft weliswaar een toezichthoudende taak en kan uit dien hoofde zelfstandig onderzoek instellen naar de wijze waarop de Wiv 2002 is uitgevoerd (artikel 78), maar dit kan slechts uitmonden in het uitbrengen van een toezichtsrapport aan de Minister (artikel 79). Daarnaast kan de CTIVD de Minister gevraagd en ongevraagd adviseren en heeft zij een adviserende rol bij de behandeling van klachten (artikel 64 lid 2). Enige rechtstreekse betrokkenheid bij het tappen van advocaten heeft de CITVD niet, zij heeft bijvoorbeeld ook niet de bevoegdheid het tappen van een advocaat te (doen) beëindigen. De omstandigheid dat binnen de diensten beleidsmatig*

[28] Rb. Den Haag 1 juli 2015, ECLI:NL:RBDHA:2015:7436.
[29] Hof Den Haag 27 oktober 2015, ECLI:NL:GHDHA:2015:2881.
[30] Rb. Den Haag 1 juli 2015, ECLI:NL:RBDHA:2015:7436, r.o. 4.11

> *zekere waarborgen in acht worden genomen bij het tappen van advocaten en het uitwerken van onderschept materiaal, doet hier niet aan af. Het gaat daarbij immers niet om een vorm van onafhankelijk toezicht.*[31]

53. Rechtbank en hof aarzelen niet om de Staat een positieve verplichting op te leggen, een en ander onder verwijzing naar de overvloedige jurisprudentie van het EHRM. De Staat krijgt zes maanden om – ter nadere bescherming van het verschoningsrecht en daarmee van het recht op een effectieve verdediging en de toegang tot het recht – het beleid voor het afluisteren van advocaten bij te stellen door een onafhankelijke toetsing in te voeren en moet anders elk tappen, afluisteren, registreren van communicatie tussen advocaten en hun cliënten staken.

Toezichtrapport CTIVD over de samenwerking van de MIVD met buitenlandse diensten

54. In navolging van het eerdere rapport over de samenwerking van de AIVD met buitenlandse inlichtingen- en veiligheidsdiensten (rapport 22a, **productie 10**), verschijnt op 10 juni 2015 het toezichtsrapport over de samenwerking van de MIVD met buitenlandse diensten.[32]

55. In het rapport constateert de CTIVD dat de MIVD gegevens uitwisselt met een groot aantal diensten over allerlei onderwerpen, variërend van algemene rapportages tot concrete informatie over personen of organisaties. De MIVD ontvangt, gevraagd en ongevraagd, ook gegevens van buitenlandse diensten.[33] Volgens de MIVD wordt het ongevraagd ontvangen van informatie steeds belangrijker.

> *De gegevens die de MVID ontvangt, hebben deels een basis in verzoeken van de MIVD aan buitenlandse diensten of bredere afspraken tussen diensten om dergelijke gegevens te ontvangen. Deels gaat het hier ook om ongevraagd verstrekte gegevens. Dit ongevraagd verstrekken van gegevens wordt steeds belangrijker, zeker bij onderwerpen waarnaar door veel buitenlandse diensten onderzoek wordt verricht, zoals de bestrijding van terrorisme en piraterij, en in het kader van crisisbeheersingsoperaties in coalitieverband. In sommige gevallen zijn hiervoor afgeschermde digitale netwerken opgericht die deling van gegevens onder een aantal diensten mogelijk maakt.*[34]

56. In het rapport en de bijlage gaat de CTIVD in op het juridisch kader voor samenwerking, neergelegd in artikel 59 Wiv. De Commissie constateert dat de Wiv een algemene zorgplicht voor samenwerking bevat en daarnaast de *verstrekking* van gegevens aan buitenlandse diensten regelt. Over het ontvangen is niets geregeld, aldus de CTIVD, waarmee zij dus erkent dat ten aanzien daarvan ook geen specifieke waarborgen bestaan. De CTIVD merkt wel op dat dit niet betekent dat dergelijke activiteiten zonder meer geoorloofd zijn.

---

[31] Hof Den Haag 27 oktober 2015, ECLI:NL:GHDHA:2015:2881, r.o. 2.8.
[32] Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen en/of veiligheidsdiensten, 10 juni 2015, CTIVD nr. 22B.
[33] Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen en/of veiligheidsdiensten, 10 juni 2015, CTIVD nr. 22B, p. 4, 24.
[34] Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen en/of veiligheidsdiensten, 10 juni 2015, CTIVD nr. 22B, p. 31.

> *Andere aspecten van de samenwerking zijn niet expliciet geregeld in de Wiv 2002. Zo zijn er geen bepalingen opgenomen over het ontvangen van gegevens, over het doen van verzoeken om ondersteuning aan buitenlandse diensten of over het uitvoeren van gezamenlijke operaties. Dit betekent niet dat dergelijke activiteiten zonder meer kunnen plaatsvinden.*[35]

57. Wat dat inhoudt, blijkt later in het rapport.

> *Bij al deze vormen van gegevensuitwisseling moet de MIVD zich telkens afvragen of de verstrekking van die specifieke gegevens aan die specifieke dienst(en) in dat specifieke geval geoorloofd is. […] Ook bij het gebruik van ontvangen gegevens moet de MIVD zich afvragen of dit geoorloofd is.*

58. De MIVD moet zich dus afvragen of zij ontvangen gegevens mag gebruiken. In de praktijk komt dit neer op een afweging. De vraag of de buitenlandse diensten die de gegevens heeft verstrekt, deze rechtmatig heeft verkregen, is daarbij nadrukkelijk van belang, aldus de Commissie. De CTIVD herhaalt in dit verband haar eerdere standpunt dat onze diensten zich moeten verdiepen in de technische mogelijkheden van bondgenoten.

> *[D]e MIVD [moet] bepaalde afwegingen maken, voordat hij gegevens kan gebruiken die (ongevraagd) ontvangen zijn van een buitenlandse dienst. […] Ook de vraag of de buitenlandse dienst die de gegevens verstrekt, deze rechtmatig heeft verkregen, is van belang bij het ontvangen van gegevens door MIVD. Zoals de Commissie ook al aankaartte in haar rapport 38, moet de MIVD in het bijzonder alert zijn op aanwijzingen die aanleiding geven te twijfelen aan de rechtmatigheid van de verwerving van de gegevens door de buitenlandse dienst. In dit verband wijst de Commissie nogmaals op het belang van voldoende informatie over de wettelijke bevoegdheden en (technische) mogelijkheden van buitenlandse diensten.*[36]

59. In de juridische bijlage bij het rapport herhaalt de Commissie haar standpunt dat bij het ongevraagd ontvangen van gegevens door de MIVD de vraag of die gegevens door de buitenlandse dienst rechtmatig zijn verkregen een belangrijke rol toekomt. De CTIVD voegt hieraan aan toe dat de MIVD "bij het ongevraagd ontvangen van gegevens in het bijzonder alert [dient] te zijn op aanwijzingen die aanleiding geven te twijfelen aan de rechtmatigheid van de verwerving van de gegevens door de buitenlandse dienst."[37]

60. Dit alles duidt op een verplichting van de Staat om zich te vergewissen van de wijze van vergaring door buitenlandse diensten, iets wat de Staat naar eigen zeggen niet kan. Hoe kan zij

---

[35] Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen en/of veiligheidsdiensten, 10 juni 2015, CTIVD nr. 22B, p. 13. Zie ook Juridische Bijlage bij het toezichtrapport over de samenwerking van de MIVD met buitenlandse inlichtingen en/of veiligheidsdiensten, *Het kader voor samenwerking met buitenlandse diensten*, p. 20: "Het ongevraagd ontvangen van gegevens is evenmin geregeld in de wet".
[36] Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen en/of veiligheidsdiensten, 10 juni 2015, CTIVD nr. 22B, p. 32.
[37] Juridische Bijlage bij het toezichtrapport over de samenwerking van de MIVD met buitenlandse inlichtingen en/of veiligheidsdiensten, *Het kader voor samenwerking met buitenlandse diensten*, p. 20.

zich vergewissen van de vraag of privacy (of andere mensenrechten) schendingen plaatsvinden als zij uit principe nooit navraag doet naar de gebruikte methoden?

Rapport Commissioner for Human Rights van de Council of Europe

61. In mei 2015 publiceert de Commissioner for Human Rights van de Europese Raad het rapport (issue paper) *Democratic and effective oversight of national security services*, waarin wordt ingegaan op de nationale vereisten waaraan moet zijn voldaan om grondrechten effectief te beschermen en inlichtingendiensten ter verantwoording te kunnen roepen.

62. Het rapport gaat onder meer in op de implicaties voor de uitingsvrijheid van internationale samenwerking en de uitwisseling van gegevens die daar deel van uitmaakt. Het rapport gaat nadrukkelijk ook in op het risico dat – bewust of onbewust – nationale waarborgen worden omzeild doordat gegevens worden ontvangen van buitenlandse diensten.

> *[C]ross-border exchanges of personal data by security services also have implications for the right to privacy. This right is engaged each time personal data are transmitted. […] A further issue is the deliberate or accidental use of international intelligence sharing to circumvent the safeguards that would ordinarily apply to the collection of information. While security services would usually have to obtain a warrant to, for example, intercept a person's communications within their country, if this same information were gathered by a foreign partner and later shared it is possible that no such safeguards would apply. Such risks are heightened in the context of intelligence sharing relationships that include automated sharing of electronic data and/or integrated systems collecting and storing information gathered by more than one state.*[38]

63. In het rapport wordt overwogen dat "it is essential that overseers are able to scrutinise information about [international co-operation between security services], including information that has been received from or sent to foreign bodies."[39]

Overige ontwikkelingen

64. In april 2014 neemt de Tweede Kamer tijdens een plenair debat over het afluisteren door de NSA twee moties aan. In motie nr. 89[40] wordt de regering verzocht te komen tot een nadere invulling van de criteria voor samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten. In motie nr. 96 constateert de Kamer dat structureel sets (meta)gegevens worden uitgewisseld aan buitenlandse inlichtingen- en veiligheidsdiensten en verzoekt de regering dit alleen te laten plaatsvinden nadat toestemming is verkregen van de betrokken minister.[41] De CTIVD kondigt naar aanleiding daarvan in juli 2015 een kortlopend onderzoek aan naar de wijze waarop de AIVD en de MIVD invulling geven aan deze moties van de Tweede Kamer. De resultaten van dit onderzoek zijn nog niet openbaar.

---

[38] Issue paper published by the Council of Europe Commissioner for Human Rights, *Democratic and effective oversight of national security services*, mei 2015, p. 24. Te vinden op: www.commissioner.coe.int.
[39] Issue paper published by the Council of Europe Commissioner for Human Rights, *Democratic and effective oversight of national security services*, mei 2015, p. 10, 64.
[40] *Kamerstukken II* 2013/14, 30 977, nr. 89.
[41] *Kamerstukken II* 2013/14, 30 977, nr. 96.

65. Op 21 april 2015 neemt het Parliamentary Assembly van de Raad van Europa unaniem een resolutie aan over “mass surveillance”.[42] Daarin erkent zij de noodzaak tot trans-Atlantische samenwerking in de strijd tegen terrorisme, maar geeft zij wel aan dat het vertrouwen in de Amerikanen een ernstige deuk heeft opgelopen na alle Snowden-onthullingen:

> *12. The Assembly also recognises the need for transatlantic cooperation in the fight against terrorism and other forms of organised crime. But it considers that such cooperation must be based on mutual trust based on respect for human rights and the rule of law. This trust has been severely damaged by the mass surveillance practices revealed in the Snowden files.*

66. Dit vertrouwen kan volgens de commissie slechts worden hersteld door te voorzien in “a legal framework [...] at the national and international level which ensures the protection of human rights, especially that which secures the right to privacy.” In dat verband roept de Assembly lidstaten op te voorzien in een internationale “intelligence codex”, waarin duidelijke regels zijn neergelegd over de samenwerking en wat daarbinnen wel en niet geoorloofd is.

67. Een andere relevante ontwikkeling, ten slotte, is dat de NSA op 28 november 2015 een klein beetje heeft moeten inleveren op de bevoegdheid tot het verzamelen van metadata van telefoongesprekken. Op die datum liep de zogenaamde Patriot Act af en trad de zogenaamde Freedom Act in werking. Die Freedom Act bevat iets meer waarborgen dan haar voorganger, want de telefoongegevens worden voortaan opgeslagen bij de telecomproviders. De NSA krijgt daar toegang toe via een (geheime) machtiging van het FISA Court. Het betreft echter een bescheiden wijziging, zo concludeert *The Guardian*. Andere grootschalige en niet-gerichte surveillance- en onderscheppingsbevoegdheden van de NSA blijven ongewijzigd:

> *Instead of being held directly by the NSA, phone data will remain with the telecom companies. The NSA will have to go to the Fisa court to get access. [...]*
> *It is a first step but a modest one. The problem – and it is a major one – is the reform applies only to phone records. The NSA can continue to harvest bulk communications from the internet and social media.*[43]

GRIEVEN

Grief 1 - Eisers

Ten onrechte overweegt de rechtbank in r.o. 5.2:

> “*Gelet op het karakter en de inhoud van de activiteiten waarop de eisende partijen-natuurlijke personen zich toeleggen, in samenhang bezien met de omstandigheid dat deze eisende partijen nationaal en internationaal in meer of mindere mate bekendheid genieten op het terrein waarop zij werkzaam zijn, acht de rechtbank aannemelijk dat deze eisers, meer dan de gemiddelde burger in Nederland, de verdenking op zich kunnen laden dat zij door hun*

[42] Parliamentary Assembly, Resolution 2045 (2015) on Mass surveillance, aangenomen op 21 april 2015.
[43] http://www.theguardian.com/us-news/2015/nov/28/nsa-bulk-metadata-collection-expires-usa-freedom-act.

activiteiten een gevaar voor de nationale veiligheid zouden kunnen opleveren en derhalve op grond van de Wiv 2002 onderwerp zouden kunnen zijn van onderzoek door de diensten."

Toelichting

68. Eisers hebben aangevoerd dat zij, gezien hun werkzaamheden en/of de activiteiten die zij ontplooien, onderwerp van onderzoek zouden kunnen van (Amerikaanse) inlichtingen- en veiligheidsdiensten (Dv 7-17). De rechtbank oordeelt – terecht – dat dit inderdaad het geval is.

69. Eisers leveren echter geen *gevaar* op voor de nationale veiligheid, noch zijn er omstandigheden die deze verdenking op zich kunnen laden. Voor zover de rechtbank dat bedoeld heeft in bovengenoemde passage, betwisten eisers dat nadrukkelijk. Bedoeld zal echter zijn – en dat hebben eisers ook aangevoerd – dat het in de rede ligt dat eisers sneller onderwerp zullen zijn van surveillance.

Grief 2 – Activiteiten buitenlandse diensten

Ten onrechte overweegt de rechtbank in r.o. 5.16:

"*De Staat heeft zich hiertegen verweerd met de stelling dat er geen aanwijzingen zijn dat buitenlandse diensten informatie aan de diensten hebben verschaft, die door die buitenlandse diensten zijn verzameld door middel van een inbreuk op de Nederlandse rechtssfeer of soevereiniteit. Voorts heeft de Staat betoogd, met een beroep op het rapport van de CTIVD van 5 februari 2014, dat er geen aanwijzingen zijn dat buitenlandse diensten met medewerking van de AIVD of de MIVD zelfstandig toegang hebben gekregen tot Nederlandse telefoon- of internetverbindingen, dat er geen sprake is van het stelselmatig door de diensten buiten de Nederlandse wet- en regelgeving om verwerven van persoonsgegevens of andere gegevens en ten slotte dat er geen aanwijzingen zijn dat de AIVD of de MIVD expliciet verzoeken aan buitenlandse diensten hebben gedaan om bevoegdheden in te zetten die volgens de Nederlandse wet- en regelgeving niet zijn toegestaan (de eerdergenoemde U-bochtconstructie). Deze verweren zijn onweersproken gebleven, zodat de rechtbank bij haar beoordeling de door de Staat genoemde feitelijke constateringen tot uitgangspunt neemt. Voor zover de vorderingen van eisers zijn gebaseerd op de stelling dat de Staat in strijd handelt met de Wiv 2002, los van artikel 8 (en artikel 10) EVRM, stuiten die vorderingen hierop af*."

Toelichting

70. Ten onrechte neemt de rechtbank in bovengenoemde overweging als uitgangspunt dat er geen aanwijzingen zijn dat buitenlandse diensten informatie aan de Nederlandse diensten hebben verschaft, die door die buitenlandse diensten zijn verzameld door middel van een inbreuk op de Nederlandse rechtssfeer of soevereiniteit. Eveneens ten onrechte meent de rechtbank dat eisers deze stelling onvoldoende hebben weersproken.

71. Eisers hebben immers weldegelijk beargumenteerd dat het niet alleen aannemelijk is dat de buitenlandse diensten ook Nederlandse burgers hebben afgeluisterd/afgetapt, maar ook dat zij activiteiten ontplooien in Nederland.

72. Eisers hebben in dat verband uitgebreid verslag gedaan van alle Snowden-onthullingen en geconcludeerd dat er, gelet op de enorme schaal waarop de Amerikaanse en Britse diensten het wereldwijde internet- en telefoonverkeer, ook van bondgenoten, onderscheppen, er geen twijfel over mogelijk is dat zij ook activiteiten ontplooien in Nederland (pleitnotities eerste aanleg 12-47). Eén van de belangrijkste internetknooppunten wereldwijd is gelegen in Amsterdam (AMS-IX); bijna alle communicatie tussen de EU en de VS loopt via die hub. Het grootste Europese datacentrum van Google bevindt zich in Nederland, bij de Eemshaven, niet heel ver van Burum.[44]

73. Dat Nederland langdurig en specifiek doelwit van de NSA geweest, blijkt ook uit publicaties in *NRC Handelsblad* (**productie 7-E**). Dat de NSA actief is in Nederland, willen (en kunnen) de verantwoordelijke ministers dan ook niet ontkennen.

> *Kan ik garanderen dat niemand in de Nederlandse data vist? Nee, dat kan ik niet garanderen. Dat werd ook door anderen al gezegd.*[45]

74. Ook de conclusie van de rechtbank ten aanzien van de vraag of de Staat in strijd handelt met de Wiv, is onjuist en in ieder geval te kort door de bocht. Eisers hebben immers uitgebreid betoogd dat en waarom de handelwijze van de Staat niet alleen in strijd is met artikel 8 EVRM, maar ook met de Wiv.

75. Het enkele feit dat er (volgens de CTIVD) geen aanwijzingen zijn dat de AIVD of de MIVD expliciet *verzoeken* aan buitenlandse diensten hebben gedaan om bevoegdheden in te zetten die volgens de Nederlandse wet- en regelgeving niet zijn toegestaan (de U-bochtconstructie), zoals de rechtbank in r.o. 5.16 overweegt, is voor die conclusie in ieder geval onvoldoende. Eisers hebben immers nadrukkelijk betoogd dat ook het *ontvangen* van informatie van buitenlandse diensten, zonder dat de (on)rechtmatige herkomst daarvan geverifieerd wordt, neerkomt op een omzeiling van de Wiv (en dus op een U-bochtconstructie). Verwezen wordt naar alinea 69-75 van de dagvaarding en alinea 79 van de pleitnotities in eerste aanleg.

76. Een en ander klemt temeer nu ook de toezichthouder, de CTIVD, van mening is dat het ontvangen van gegevens door de Nederlandse diensten onrechtmatig is als het bij de Nederlandse diensten bekend is of bekend verondersteld mag worden dat deze gegevens door de buitenlandse dienst zijn verzameld op een manier die een ongeoorloofde inbreuk op de persoonlijke levenssfeer oplevert. Dat zou onacceptabel zijn, omdat dan afbreuk wordt gedaan aan de bescherming van de grondrechten waartoe de Nederlandse staat zich via internationale verdragen heeft verplicht en die onderdeel uitmaken van de belangen die de Nederlandse diensten op grond van de Wiv hebben te behartigen (**productie 8, p. xi**).[46]

77. De CTIVD heeft bovendien geconcludeerd dat enkel “vertrouwen”, in het licht van alle onthullingen, geen voldoende basis meer vormt voor gegevensuitwisseling. De diensten dienen zich op zijn minst nader te informeren over de wettelijke bevoegdheden en technische

[44] http://www.trouw.nl/tr/nl/4324/Nieuws/article/detail/3567463/2013/12/24/Nederland-kan-Silicon-Delta-worden.dhtml
[45] *Kamerstukken II*, 30 977, nr. 71, p. 26.
[46] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 65.

mogelijkheden van buitenlandse diensten (**productie 8, p. 30**). In de juridische bijlage bij het laatste toezichtsrapport concludeert de CTIVD dat de vraag of gegevens door een buitenlandse dienst rechtmatig zijn verkregen een belangrijke rol toekomst bij het ongevraagd ontvangen van gegevens.[47]

78. Voor zover volgens uw hof enige bewijslast op eisers rust, bieden zij aan hun stellingen te bewijzen met alle middelen rechtens. Dit bewijsaanbod heeft in elk geval – maar niet uitsluitend – betrekking op het bestaan van de verschillende surveillanceprogramma's van de NSA en de GCHQ, alsmede het feit dat ook Nederlandse burgers daardoor geraakt worden.

79. Voor zover de Staat slaagt in het leveren van bewijs van haar stellingen, bieden eisers aan tegenbewijs te leveren, eveneens door alle middelen rechtens.

Grief 3 – NSA & Nine Eyes

Ten onrechte overweegt de rechtbank in r.o. 5.19:

> *"*[...] *Ter zitting hebben eisers gesteld dat het hun in deze zaak niet gaat om de samenwerking met buitenlandse diensten als zodanig, maar om de grenzen die in het kader van deze samenwerking in acht moeten worden genomen. Nu eisers hun stellingen toespitsen op de samenwerking met de NSA, zal de rechtbank hierna in het bijzonder op die samenwerking ingaan. Nu het eisers niet om de samenwerking met de NSA als zodanig is te doen en zij onvoldoende feiten hebben gesteld die nopen tot de conclusie dat de NSA niet aan de genoemde selectiefactoren voldoet, is uitgangspunt dat de diensten op zichzelf mogen samenwerken met de NSA. Dit geldt naar het oordeel van de rechtbank ook indien Nederland deel zou uitmaken van de zogenoemde 'Nine Eyes', waarbij de rechtbank in het midden laat of dit het geval is."*

<u>Toelichting</u>

80. Ten onrechte beperkt de rechtbank de beoordeling tot de samenwerking met de Amerikaanse NSA. De vorderingen van eisers zien immers meer in zijn algemeenheid op het ontvangen en gebruiken van gegevens van buitenlandse inlichtingen- en veiligheidsdiensten die zijn verkregen in strijd met het Nederlands recht en/of één of meer van de internationale verdragsverplichtingen. Meer specifiek hebben eisers aan hun vordering nadrukkelijk ook de onthullingen rondom de Britse GCHQ ten grondslag gelegd. De Britse GCHQ is overigens gebonden aan het EHRM.

81. Eveneens ten onrechte laat de rechtbank in het midden of Nederland deel uitmaakt van de zogenaamde "Nine Eyes". Dat feit is wel degelijk relevant, omdat het iets zegt over de intensiviteit van de samenwerking, die zeer hoog is. Concreet betekent het dat Nederland als intensieve bondgenoot samenwerkt met – en gegevens uitwisselt met – partijen (de NSA en GCHQ) die op grote schaal inbreuk plegen op het recht op privacy. Voor de juridische beoordeling is dat relevant.

[47] Juridische Bijlage bij het toezichtrapport over de samenwerking van de MIVD met buitenlandse inlichtingen en/of veiligheidsdiensten, *Het kader voor samenwerking met buitenlandse diensten*, p. 20.

Grief 4 - Amerikaanse wet- en regelgeving

Ten onrechte overweegt de rechtbank in r.o. 5.20 dat de Nederlandse diensten er in het algemeen op mogen vertrouwen dat buitenlandse diensten de voor hen geldende nationale wet- en regelgeving en internationale verdragsverplichtingen respecteren. Eveneens ten onrechte overweegt de rechtbank in r.o. 5.21 dat gezien "de Amerikaanse wet- en regelgeving en het daarin vervatte systeem van toezicht op de naleving ervan" niet in zijn algemeenheid gezegd kan worden dat de Nederlandse diensten in strijd met artikel 8 EVERM handelen in het geval van de ontvangst en het gebruik van gegevens van de NSA.

Toelichting

82. In de betreffende rechtsoverwegingen oordeelt de rechtbank dat de huidige manier van samenwerken en gegevens uitwisselen met de Amerikanen niet in zijn algemeenheid in strijd is met artikel 8 EVRM, waarbij de rechtbank van belang acht dat de NSA gebonden is aan Amerikaanse regelgeving en de daarin vervatte waarborgen.

83. De overweging van de rechtbank is onjuist. De samenwerking en de gegevensuitwisseling die daarvan deel uitmaakt is wel degelijk in strijd met artikel 8 EVRM, nu daarvoor geen (afdoende) wettelijke grondslag en waarborgen voor bestaat. Verwezen zij naar de toelichting op Grief 5.

84. Voor zover de rechtbank met de betreffende overweging zou bedoelen dat de genoemde Amerikaanse regels en de daarin vervatte bevoegdheden en waarborgen, in overeenstemming zijn met internationale verdragsverplichtingen, waaronder artikel 19 IVBPR (r.o. 5.20), is dat oordeel eveneens onjuist.

85. In de eerste plaats omdat, zoals de rechtbank ook overweegt in r.o. 5.22, niet bekend is op welke wijze gegevens precies worden verzameld door de NSA. Gelet op die onduidelijkheid, kunnen überhaupt geen uitspraken worden gedaan over wat *in algemene zin* geldt en dus ook niet dat de samenwerking in algemene zin de toets van artikel 8 EVRM kan doorstaan. Eenzelfde conclusie bereikte de EU-VS werkgroep (**productie 13**).[48]

86. In de tweede plaats omdat de grootschalige en niet-gerichte surveillance- en onderscheppingsactiviteiten waar de Amerikanen (en de Britten) zich van bedienen, eenvoudigweg te ver gaan. De Snowden-onthullingen hebben duidelijk gemaakt dat de verhouding tussen de bescherming van de (inter)nationale veiligheid enerzijds, en het recht op privacy en de vrijheid van meningsuiting, bij de Amerikanen en Britten volledig zoek is. Het toezicht op de activiteiten van de inlichtingendiensten vindt plaats in het kader van een geheime procedure die niet op tegenspraak verloopt. De bevoegdheden van deze diensten zijn bovendien volstrekt disproportioneel. De Amerikanen hebben grootschalige en ongedifferentieerde toegang tot de gegevens van vrijwel de volledige Europese bevolking[49] (en een groot deel van de Amerikaanse bevolking).[50]

[48] 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.
[49] Aldus ook Ierse High Court, weergegeven in Schrems (r.o. 30-34).
[50] Vgl. paragraaf 2.3.4. van de toelichting van rapporteur Pieter Omtzigt bij de resolutie over Mass Surveillance van het Pariamentary Assembly, Doc. 13734.

87. Dat het recht en de praktijk in de VS onvoldoende waarborgen ter bescherming van de grondrechten bevat, heeft de hoogste Europese rechter met zoveel woorden bepaald in *Schrems*.[51] Het Hof sanctioneert in die zaak de gegevensuitwisseling tussen de Europese Unie en de Verenigde Staten, omdat de Verenigde Staten geen niveau van bescherming van grondrechten biedt dat in grote lijnen overeenstemt, of zelfs maar in de buurt komt van, het niveau in Europa. De Amerikaanse bevoegdheden bevatten geen waarborgen en zijn disproportioneel.

> *Niet beperkt tot het strikt noodzakelijke is dan ook een regeling die algemeen toestaat dat alle persoonsgegevens van alle personen van wie de gegevens vanuit de Unie naar de Verenigde Staten worden doorgegeven, worden bewaard, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het nagestreefde doel en zonder dat wordt voorzien in een objectief criterium ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan voor specifieke doeleinden, die strikt beperkt zijn en als rechtvaardiging kunnen dienen voor de inmenging als gevolg van zowel de toegang tot als het gebruik van deze gegevens.*[52]

88. Datzelfde vindt het VN Mensenrechtencomité, dat de praktijken van de Amerikaanse NSA veroordeelt, omdat deze niet in overeenstemming zijn met de vereisten van artikel 17 IVBPR. In het laatste periodieke rapport over de Verenigde Staten overweegt zij dat de surveillance-praktijken van de Amerikanen grotendeels geheim zijn en daardoor onvoorzienbaar. Ook de bestaande toezichtmechanismen schieten tekort. Het VN Mensenrechtencomité roept de VS op aan haar verplichtingen op grond van artikel 17 IVBPR te voldoen.[53]

> *The State party should:*
> *(a) Take all necessary measures to ensure that its surveillance activities, both within and outside the United States, conform to its obligations under the Covenant, including article 17; in particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance;*
> *(b) Ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that: (i) are publicly accessible; (ii) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (iii) are sufficiently precise and specify in detail the precise circumstances in which any such interference may be permitted, the procedures for authorization, the categories of persons who may be placed under surveillance, the limit on the duration of surveillance; procedures for the use and storage of data collected; and (iv) provide for effective safeguards against abuse;*

[51] Zie Conclusie van Advocaat-Generaal Y. Bot van 23 september 2015, Zaak C 362/14 (*Schrems*), ov. 25, 35-36, 45, 155.
[52] HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*), r.o. 93.
[53] Overigens is het Mensenrechtencomité al net zo kritisch over de GCHQ, zie United Nations Human Rights Committee, Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland, 17 augustus 2015, CCPR/C/GBR/CO/7, paragraaf 24.

> *(c) Reform the current oversight system of surveillance activities to ensure its effectiveness, including by providing for judicial involvement in the authorization or monitoring of surveillance measures, and considering the establishment of strong and independent oversight mandates with a view to preventing abuses;*
> *(d) Refrain from imposing mandatory retention of data by third parties;*
> *(e) Ensure that affected persons have access to effective remedies in cases of abuse.*[54]

89. Uit de reactie van Amerikanen blijkt wel hoe serieus zij deze aanbevelingen nemen:

> *The Committee's recommendation implies that an interference under Article 17 has to be essential or necessary and be proportionate to achieve a legitimate objective. The United States notes that these legal concepts are derived from certain regional jurisprudence, are not broadly accepted internationally, go beyond that which is required by the text of Article 17, and are not supported by the travaux of the treaty. The United States again asserts its longstanding position that obligations under the Covenant apply only with respect to individuals who are both within the territory of the State Party and within its jurisdiction.*[55]

90. In de derde plaats omdat de Amerikaanse regelgeving uitgaat van een geheel andere notie van privacy, zoals ook de rechtbank terecht overweegt in r.o. 5.22. Dat blijkt wel uit het feit dat het metadataprogramma voor telefoongegevens is vervangen door een systeem van dataretentie, waarbij de data wordt opgeslagen bij de bedrijven die ze verwerken, om eventueel later te kunnen worden opgevraagd. Een dergelijke systeem van dataretentie is in 2014 door het HvJEU als ongrondwettig bestempeld. De nationale veiligheid – hoe belangrijk ook – kan een dergelijke algemene bewaring van de gegevens van iedereen, verdacht of onverdacht, niet rechtvaardigen (**productie 38**).[56]

91. Het HvJEU is niet de enige die vindt dat wat de Amerikanen en Britten doen, te ver gaat. Minister Plasterk heeft zelf ook aangegeven dat het rondshoppen op internet, zoals de Amerikanen doen, in strijd is met het recht op privacy. Het Europees Parlement (**productie 15**) en de Werkgroep 29 (**productie 16**) veroordelen de werkwijze en de methodes van de Amerikaanse diensten in felle bewoordingen. De CTIVD adviseert onze diensten om de samenwerking met en het vertrouwen in de NSA te herzien, omdat het in het licht van de Snowden-onthullingen gewenst is om na te gaan of dit vertrouwen nog steeds terecht is (**productie 8**).Die aanbeveling herhaalt zij in het toezichtsrapport over de samenwerking van de MIVD met buitenlandse diensten.[57]

---

[54] United Nations Human Rights Committee, *Concluding observations on the fourh periodic report of the United States of America*, 23 April 2014, CCPR/C/USA/CO/04, para. 22.
[55] One-Year Follow-up Response of the United States of America to Priority Recommendations of the Human Rights Committee on its Fourth Periodic Report on Implementation of the International Covenant on Civil and Political Rights, p. 12. Te vinden op: http://www.state.gov/documents/organization/242228.pdf.
[56] HvJEU 8 april 2014, zaken C-293/12 en C-594/12 (*Digital Rights Ireland*), r.o. 51.
[57] Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen en/of veiligheidsdiensten, 10 juni 2015, CTIVD nr. 22B, p. 11.

92. Gezien al het voorgaande had de rechtbank niet mogen oordelen dat de diensten er in het algemeen op mogen vertrouwen dat buitenlandse diensten hun internationale verdragsverplichtingen respecteren. De rechtbank had het tegenovergestelde moeten oordelen.

Grief 5 – Voorzienbaarheid

Ten onrechte heeft de rechtbank in de overwegingen 5.25-5.33, samengevat, geoordeeld dat er bij internationale samenwerking op het gebied van geheime surveillance aanleiding bestaat voor een minder stringente, invulling van de eisen die artikel 8 lid 2 EVRM stelt aan de rechtvaardiging van een inbreuk op de persoonlijke levenssfeer, in het bijzonder wat betreft het vereiste dat de beperking van de bescherming van de persoonlijke levenssfeer bij wet voorzien moet zijn. Eveneens ten onrechte overweegt de rechtbank dat in dat geval minder stringente waarborgen zijn vereist.

Toelichting

93. Deze grief richt zich tegen het samenstel van overwegingen van de rechtbank met betrekking tot het zogenaamde "voorzienbaarheidsvereiste", neergelegd in artikel 8 lid 2 EVRM en artikel 52 van het Handvest. De rechtbank overweegt dat de bestaande rechtspraak van het EHRM niet zonder meer moet worden doorgetrokken naar verzameling van (ruwe) gegevens in bulk in het kader van internationale samenwerking tussen inlichtingen en- veiligheidsdiensten (r.o. 5.28). De strenge eisen van voorzienbaarheid gelden volgens de rechtbank niet bij internationale samenwerking op het gebied van geheime surveillance (r.o. 5.29). Deze veronderstelling wordt in de overwegingen 5.30-5.33 uitgewerkt. De rechtbank acht met name van belang dat het gaat om de uitwisseling van (ruwe) gegevens in bulk (r.o. 5.31 en 5.33).

94. Waar de rechtbank had moeten onderzoeken of artikel 59 van de Wiv een voldoende wettelijke grondslag biedt voor het ontvangen en gebruiken van informatie die buitenlandse diensten (in strijd met internationale verdragsverplichtingen hebben verzameld), laat de rechtbank het antwoord op die belangrijke vraag in het midden. Hoewel de rechtbank suggereert dat artikel 59 Wiv niet onder alle omstandigheden de toets van artikel 8 lid 2 EVRM kan doorstaan, volstaat zij met het oordeel dat "zodanig verstrekkende waarborgen als eisers voorstaan", niet vereist zijn (r.o. 5.28).

95. De overwegingen van de rechtbank zijn onjuist om de volgende redenen, in onderling verband beschouwd, die hieronder nader zullen worden uitgewerkt:

- Het voorzienbaarheidsvereiste wordt niet afgezwakt in het kader van geheime surveillance. Integendeel. Tegenover het heimelijke karakter van geheime bevoegdheden en het gebrek aan democratische controle, moeten volgens het EHRM juist strenge waarborgen staan;
- Uit *Liberty* en *Weber* vloeit juist voort dat de in die arresten geformuleerde minimum normen van toepassing zijn in zaken zoals deze, die de uitwisseling van ongericht verzamelde en grote hoeveelheden data betreft;
- Zelfs als de door de rechtbank geformuleerde norm zou volstaan, is daar in casu niet aan voldaan.

Artikel 8 EVRM

96. Zoals de rechtbank terecht vooropstelt (r.o. 5.25), strekt het toepassingsbereik van artikel 8 EVRM zich – onder meer – uit tot het verzamelen (intercepteren) en het verwerken en opslaan van persoonsgegevens en metadata (ook wel verkeersgegevens). Dat geldt ook voor het onderscheppen van communicatie en het registreren van gedragingen van mensen op het internet. Ook het opslaan van gegevens over het privéleven van burgers in geheime overheidsdatabases heeft het EHRM onder de reikwijdte van artikel 8 EVRM gebracht.[58] Zelfs het enkele bestaan van wetgeving die dergelijke bevoegdheden toekent aan inlichtingen- en veiligheidsdiensten, levert reeds een inbreuk op artikel 8 op.[59]

97. Ook de samenwerking tussen diensten en de uitwisseling van informatie die daar onderdeel van uitmaakt, is een beperking van het recht op privacy die ten volle moet worden getoetst aan artikel 8 EVRM.[60] Het EHRM heeft dat nadrukkelijk bevestigd in de zaak *Weber en Saravia*:

> *Furthermore, the Court, like the Federal Constitutional Court, takes the view that the transmission of data to and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, constitutes a further separate interference with the applicants' rights under Article 8* […] (**productie 34**).[61]

98. Beperkingen van het recht op privacy zijn op grond van het tweede lid van artikel 8 EVRM slechts gerechtvaardigd voor zover deze bij wet zijn voorzien en in een democratische samenleving noodzakelijk zijn in het belang van– onder meer – de nationale veiligheid.

99. Volgens vaste jurisprudentie van het EHRM brengt het vereiste dat een beperking bij wet moet zijn voorzien, met zich mee dat die beperking gebaseerd moet zijn op een nationale wettelijke regel, die voldoende toegankelijk ("accessible") is voor de betrokkene en voldoende voorzienbaar ("foreseeable") is.[62]

> *In the Court's opinion, the following are two of the requirements that flow from the expression 'prescribed by law'. Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able — if need be with appropriate advice — to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.*[63] (onderstreping advocaat)

[58] EHRM 24 mei 2011 (*Association "21 Decembre 1989" e.a/Roemenië*), r.o. 115.
[59] EHRM 29 juni 2006 (*Weber & Saravia*), r.o. 78, onder verwijzing naar EHRM 6 september 1978 (*Klass/ Germany*), r.o. 41 en EHRM 2 augustus 1984 (*Malone/ UK*), r.o. 64, EHRM 16 februari 2002 (*Amann/Zwitserland*), r.o. 65, EHRM 4 mei 2000 (*Rotaru/Roemenië*), r.o. 43.
[60] Issue paper published by the Council of Europe Commissioner for Human Rights, Democratic and effective oversight of national security services, mei 2015, p. 24
[61] EHRM 29 juni 2006 (*Weber & Saravia*), r.o. 77.
[62] Zie het rapport van de Research Division van het EHRM, *National security and European case-law*, 2013, p. 7.
[63] EHRM 26 april 1979, *NJ* 1980, 146 (*Sunday Times*), r.o. 49.

Waarborgen essentieel in zaken betreffende geheime surveillance

100. De rechtbank stelt in r.o. 5.26 dat het EHRM de eis van voorzienbaarheid in het kader van geheime surveillance “afzwakt”, omdat de inzet van dergelijke geheime maatregelen noodzakelijk gedeeltelijk onvoorzienbaar moet blijven.

101. Dit verstrekkende standpunt van de rechtbank vindt geen steun in het recht. De rechtbank baseert deze overweging vermoedelijk op de rechtspraak van het EHRM, waarin is bepaald dat het voorzienbaarheidsvereiste in de context van heimelijke operaties niet zo ver gaat dat een individu moet kunnen voorzien wanneer zijn communicatie onderschept zal worden, zodat hij zijn gedrag daarop kan afstemmen.

> *Foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly.*[64]

102. Eisers hebben dit, anders dan de rechtbank overweegt (r.o. 5.26), onder verwijzing naar de rechtspraak van het EHRM, ook onderkend (zie Dv 57, pleitnotities 68)

103. Dat het karakter van surveillance maatregelen door inlichtingen- en veiligheidsdiensten een zekere onvoorzienbaarheid noodzakelijk maakt, betekent niet dat het “voorzien bij wet”-vereiste *als zodanig* ook mag worden “afgezwakt” wanneer het geheime diensten betreft. Met name betekent het niet dat de wettelijke grondslag ook minder waarborgen zou moeten bevatten, zoals de rechtbank overweegt in r.o. 5.28 en 5.29:

> *Zodanig vérstrekkende waarborgen als eisers voorstaan, eist artikel 8 lid 2 EVRM naar het oordeel van de rechtbank bij de ontvangst en het gebruik van gegevens in het kader van internationale samenwerking zoals door eisers gesteld, evenwel niet.*
>
> *Bij internationale samenwerking op het gebied van geheime surveillance bestaat er naar het oordeel van de rechtbank temeer aanleiding voor een bijzondere, dat wil zeggen minder stringente, invulling van de eisen die artikel 8 lid 2 EVRM stelt aan de gerechtvaardigdheid van een inbreuk op de persoonlijke levenssfeer van het individu, in het bijzonder wat betreft de voorzienbaarheid van de nationale wetgeving.*

104. Dit is een zeer verstrekkend oordeel van de rechtbank, zonder juridische basis. Het tegendeel is immers rechtens juist. Het EHRM heeft juist aangenomen dat, omdat bij heimelijke bevoegdheden het risico op willekeur erg groot is en de werkwijze van geheime diensten zich onttrekt aan democratische controle, duidelijke en gedetailleerde regels over de toelaatbaarheid van dergelijke bevoegdheden essentieel zijn. Om die reden vereist het EHRM dat de reikwijdte en uitvoeringsmodaliteiten van de wettelijke bepaling die de grondslag biedt voor de heimelijke maatregelen voldoende duidelijk is en dat er adequate en effectieve (procedurele) waarborgen bestaan tegen willekeur. Die waarborgen en het belang daarvan worden in de rechtspraak van het EHRM consequent benadrukt.

[64] Zie onder meer EHRM 2 augutus 1984 (*Malone/UK*), r.o. 67, EHRM 26 maart 1987 (*Leander/Zweden*), r.o. 51.

> *[…] this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate. The Court must be satisfied that, whatever system is adopted, there exist adequate and effective guarantees against abuse.*[65]

> *Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident. […] Undoubtedly, as the Government rightly suggested, the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. […] Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.*[66]

105. De wettelijke grondslag mag ook niet zodanig zijn geformuleerd dat zij een vrijwel onbeperkte discretionaire bevoegdheid toekennen aan de uitvoerende macht of aan de rechter.

> *[S]since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.*[67]

106. Waarborgen worden volgens het EHRM alleen maar belangrijker naarmate de beschikbare technologie geavanceerder wordt en de verzamelde persoonsgegevens in steeds grotere mate geautomatiseerd worden verwerkt.

> *It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated.* [68]

> *The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for*

[65] EHRM 6 september 1978 (*Klass/ Germany*), r.o. 49.
[66] EHRM 2 augustus 1984 (*Malone/ UK*), r.o. 67.
[67] Zie EHRM 2 augustus 1984 (*Malone/UK*) r.o. 68, EHRM 26 maart 1987 (*Leander/Zweden*) r.o. 51, EHRM 24 april 1990 (*Huvig/Frankrijk*) r.o. 29 en EHRM 29 juni 2006 (*Weber en Saravia/Duitsland*), r.o. 94.
[68] EHRM 29 juni 2006 (*Weber en Saravia/Duitsland*), r.o. 93, EHRM 25 maart 1998 (*Kopp/Zwitserland*), r.o. 72, EHRM 30 juli 1998 (*Valenzuele Contreras/Spanje*), r.o. 46.

police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored. [69]

107. Zeer recent, op 12 januari 2016, benadrukt het EHRM in de zaak *Szabó* nogmaals dat de potentiële inmengingen op het recht op privacy bijzonder groot en acuut zijn gelet op de hedendaagse technologische mogelijkheden. Het EHRM beklemtoont de noodzaak van waarborgen in dat verband.

> *Given the technological advances since the Klass and Others case, the potential interferences with email, mobile phone and Internet services as well as those of mass surveillance attract the Convention protection of private life even more acutely (see Copland v. the United Kingdom, no. 62617/00, § 41, ECHR 2007 I).*[70]
>
> *For the Court, it is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents. The techniques applied in such monitoring operations have demonstrated a remarkable progress in recent years and reached a level of sophistication which is hardly conceivable for the average citizen (see the CDT's submissions on this point in paragraphs 49-50 above), especially when automated and systemic data collection is technically possible and becomes widespread. In the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights. […] Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. In this context the Court also refers to the observations made by the Court of Justice of the European Union and, especially, the United Nations Special Rapporteur, emphasising the importance of adequate legislation of sufficient safeguards in the face of the authorities' enhanced technical possibilities to intercept private information (see paragraphs 23 and 24 above).*[71]

108. Het EHRM verwijst in haar recente rechtspraak nadrukkelijk ook naar de Digital Rights-uitspraak van het HvJEU,[72] waarin eveneens het grote belang van waarborgen wordt benadrukt.[73] In het latere arrest *Schrems* ging om het uitwisselen van data door Europese

[69] EHRM 4 december 2008 (*S. and Marper/UK*), r.o. 103, EHRM 18 oktober 2011 (*Khelili/Zwitserland*), r.o. 62.
[70] EHRM 12 januari 2016 (*Szabó en Vissy/Hongarije*), r.o. 53.
[71] EHRM 12 januari 2016 (*Szabó en Vissy/Hongarije*), r.o. 68.
[72] EHRM 4 december 2015 (Roman Zakharov/Rusland), r.o. 147, EHRM 12 januari 2016 (Szabó & Vissy/Hongarije), r.o. 23, 68, 70, 73.
[73] HvJEU 8 april 2014, zaken C-293/12 en C-594/12 (*Digital Rights Ireland*, r.o. 54, waar het HvJEU met zoveel woorden verwijst naar de rechtspraak van het EHRM.

bedrijven met de Amerikanen. Het HvJEU oordeelt dat een regeling die een inmenging van het recht op privacy met zich meebrengt, duidelijke en precieze regels betreffende de draagwijdte en de toepassing van een maatregel dient te bevatten, zodat de personen die erdoor getroffen worden, over voldoende garanties beschikken en worden beschermd tegen misbruik en onrechtmatige raadplegingen.

> *Wat het binnen de Unie gewaarborgde niveau van bescherming van de grondrechten en fundamentele vrijheden betreft, moet een regeling van de Unie die een inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten met zich brengt, volgens vaste rechtspraak van het Hof duidelijke en precieze regels betreffende de draagwijdte en de toepassing van een maatregel bevatten en minimale vereisten opleggen, zodat de personen van wie de persoonsgegevens aan de orde zijn, over voldoende garanties beschikken dat hun gegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens. De noodzaak om over dergelijke garanties te beschikken is des te groter wanneer de persoonsgegevens automatisch worden verwerkt en er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd (arrest Digital Rights Ireland e.a., C 293/12 en C 594/12, EU:C:2014:238, punten 54 en 55 en aldaar aangehaalde rechtspraak).*[74] (onderstreping advocaat).

109. De Safe Harbor beschikking voorziet volgens het HvJEU niet in de vereiste waarborgen en beperkt de bevoegdheid ook niet tot het strikt noodzakelijke.

110. Waarborgen, die de burger beschermen tegen misbruik en willekeur, zijn dus essentieel, juist op het terrein van regelgeving in het kader van de nationale veiligheid en juist ook wanneer het de uitwisseling van informatie met buitenlandse diensten betreft. De burger moet kunnen begrijpen onder welke omstandigheden de overheid een bepaalde inbreukmakende bevoegdheid mag uitoefenen en onder welke voorwaarden.[75] Daarnaast hecht het EHRM aan de aanwezigheid van adequate juridische procedures om vermeende willekeurige inmengingen aan te kunnen vechten.[76]

Toepasselijkheid minimumwaarborgen

111. In de zaak *Weber en Saravia* heeft het EHRM bovengenoemde uitgangspunten vertaald naar een aantal minimumwaarborgen waaraan een nationale wettelijke regeling moet voldoen. Wil voldaan zijn aan het voorzienbaarheidsvereiste, dan moet volgens het EHRM in ieder geval duidelijk zijn:

    i. welke (dreigende) activiteiten aanleiding kunnen geven voor de interceptie van telecommunicatie (de “nature of the offences”);
    ii. welke categorieën van personen (“categories of people”) kunnen worden getroffen door de interceptiebevoegdheid;

[74] HvJEU 6 oktober 2015, zaak 362/14 (*Schrems*), ro. 91.
[75] EHRM 2 augustus 1984 (*Malone/ UK*), r.o. 68 EHRM 24 april 1990 (*Kruslin/ France*), r.o. 33 en 35.
[76] EHRM 4 mei 2000 (*Rotaru/Roemenië*), r.o. 59.

iii. wat de maximale duur is van de interceptiebevoegdheid (“a limit on the duration”);
iv. welke procedure moet worden gevolgd om de verkregen gegevens te mogen onderzoeken, gebruiken en opslaan (“the procedure to be followed for examing, using and storing the data obtained”);
v. welke voorzorgsmaatregelen er moeten worden getroffen bij het gebruik van de gegevens en het verschaffen daarvan aan derde partijen (“the precautions to be taken when communicating the data to other parties”); en
vi. de omstandigheden waaronder de gegevens moeten worden gewist of vernietigd (“the circumstances in which recordings may or must be erased”) (**productie 34, r.o. 95)**.

112. In *Liberty* heeft het EHRM aangegeven dat de in *Weber en Saravia* op een rij gezette voorwaarden weliswaar zijn ontwikkeld in jurisprudentie die zag op gevallen van gerichte interceptie van communicatie, maar dat het geen reden ziet om bij grootschaliger en ongerichte onderschepping van communicatie minder strikte voorwaarden te hanteren.[77]

113. Volgens de rechtbank (r.o. 5.28) kunnen deze waarborgen echter niet zonder meer worden doorgetrokken naar de verzameling van (ruwe) gegevens in bulk in het kader van internationale samenwerking tussen inlichtingen- en veiligheidsdiensten (r.o. 5.28). Als reden hiervoor geeft de rechtbank dat geen van de uitspraken van het EHRM betrekking had op de uitwisseling van gegevens in het kader van internationale samenwerking (r.o. 5.29)

114. Deze aanname van de rechtbank is niet juist. Zoals hierboven aangegeven, had nota bene de zaak *Weber en Saravia* zelf (mede) betrekking op de “transmission of data to and their use by other authorities”.

> *[This case] notably concerns the extension of the powers of the Federal Intelligence Service (Bundesnachrichtendienst) with regard to the recording of telecommunications in the course of so-called strategic monitoring, as well as the use (Verwertung) of personal data obtained thereby and their transmission to other authorities*.[78]

115. Die uitwisseling levert volgens het EHRM een aparte inmenging (een “further separate interference”) op, die afzonderlijk moet worden getoetst aan de (voorzienbaarheids)eisen die artikel 8 lid 2 EVRM stelt. In *Weber* constateert het EHRM dat de uitwisselingsbevoegdheid in die zaak aan de die eisen voldeed, omdat de bepaling (na aanpassing) voorzag in voldoende waarborgen, onder meer ten aanzien van de te volgen procedure, de gevallen waarin uitwisseling was toegestaan, en omdat voorzien was in onafhankelijke toezicht.

> *99. Moreover, the procedure to be followed for examining and using the data obtained was regulated in detail in section 3(3)-(5) of the amended G 10 Act. <u>In particular, section 3(3) and (5) laid down limits and precautions concerning the transmission of</u>*

[77] EHRM 1 juli 2008, *NJ* 2010, 325, m. nt. Dommering (*Liberty*).
[78] EHRM 29 juni 2006 (*Weber en Saravia/Duitsland*), r.o. 94

data to other authorities; these were further strengthened by the Federal Constitutional Court in its judgment in the instant case.[79]

122. The Court finds that the impugned provision, as amended and applicable following the judgment of the Federal Constitutional Court, laid down strict conditions with regard to the transmission to the Federal Government of data obtained by means of strategic monitoring. […] *The additional safeguards introduced by the Federal Constitutional Court are appropriate for the purpose of limiting the use of the information obtained to what is necessary to serve the purpose of strategic monitoring. […]*
125. The Court finds that the transmission of personal data obtained by general surveillance measures without any specific prior suspicion in order to allow the institution of criminal proceedings against those being monitored constitutes a fairly serious interference with the right of these persons to secrecy of telecommunications. It observes in this connection that the catalogue of offences for the investigation of which knowledge obtained by means of strategic monitoring could be used was considerably enlarged by the amendment of the G 10 Act at issue.
126. However, it notes that the use of information obtained by strategic monitoring to these ends was limited: personal data could be transmitted to other authorities merely in order to prevent or prosecute the serious criminal offences listed in section 3(3) of the amended G 10 Act.
127. Moreover, the Court observes that the Federal Constitutional Court found that the impugned section, in its version in force at the relevant time, interfered disproportionately with the secrecy of telecommunications as protected by the Basic Law. That court therefore ordered that, pending the entry into force of legislation in compliance with the Constitution, section 3(5) could only be applied and data be transmitted if specific facts – as opposed to mere factual indications – aroused the suspicion that someone had committed one of the offences listed in section 3(3). Furthermore, the transmission had to be recorded in minutes. Accordingly, that court again considerably strengthened the safeguards against abuse.
128. In addition, the decision to transmit data had to be taken by a staff member of the Federal Intelligence Service qualified to hold judicial office, who was particularly well trained to verify whether the conditions for transmission were met. Moreover, as clarified in the Federal Constitutional Court's judgment, the independent G 10 Commission's powers of review extended to verifying that the statutory conditions for data transmission were complied with.
129. In the light of the above, the Court takes the view that the interference with the secrecy of the communications made by persons subject to monitoring in accordance with the impugned provision was counterbalanced both by a reasonable limitation of the offences for which data transmission was permitted and by the provision of supervisory mechanisms against abuse.

116. Maar ook als de eerdere EHRM-zaken geen betrekking zouden hebben op de uitwisseling van (bulk)data, zoals de rechtbank ten onrechte overweegt, valt niet in te zien waarom de

[79] EHRM 29 juni 2006 (*Weber en Saravia/Duitsland*), r.o. 99.

waarborgen uit *Weber* niet zouden (moeten) gelden wanneer het de ontvangst en het gebruik van gegevens afkomstig van buitenlandse diensten betreft.

117. De Weber-eisen worden door het EHRM zelf aangeduid als “minimum safeguards against arbitrary interference”. Het betreft, met andere woorden, *minimum* vereisten waaraan volgens het EHRM in ieder geval moet zijn voldaan.

118. Niet voor niets worden de Weber-waarborgen in de rechtspraak van het EHRM ook consequent herhaald en toegepast, in een veelheid van situaties die raken aan surveillance. In latere EHRM-arresten worden deze eisen doorgaans als volgt samengevat:

> *[B]ecause of the lack of public scrutiny and the risk of abuse intrinsic to any system of secret surveillance, the following minimum safeguards should be set out in statute law to avoid abuses: the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law.*[80]

119. Ook recent heeft het EHRM deze minimumwaarborgen weer herhaald en toegepast, in de zaken *Roman Zakharov* en *Szabó*.[81]

> *56. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in law in order to avoid abuses of power: the nature of offences which may give rise to an interception order; the definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed (see Huvig v. France, 24 April 1990, § 34, Series A no. 176 B; Amann v. Switzerland [GC], no. 27798/95, §§ 56-58, ECHR 2000 11; Valenzuela Contreras v. Spain, 30 July 1998, § 46, Reports 1998 V; Prado Bugallo v. Spain, no. 58496/00, § 30, 18 February 2003; Weber and Saravia, cited above, § 95; Association for European Integration, cited above, § 76; and Roman Zakharov, cited above, § 231).*[82]

120. Het is niet in te zien waarom de bevoegdheid tot het ontvangen en gebruiken van verzamelde (bulk)data van buitenlandse diensten, aan lagere standaarden zou moeten voldoen, zoals de rechtbank meent (r.o. 5.28). Temeer nu het daarbij juist gaat om (de uitwisseling van) gegevens die zijn verkregen door middel van grootschalige en ongerichte onderschepping van communicatie (in bulk), waar *Liberty* op ziet en ten aanzien waarvan het EHRM dus juist heeft geoordeeld dat er geen reden is om minder strikte voorwaarden te hanteren.

[80] EHRM 21 juni 2011 (*Shimovolos/Rusland*), r.o. 68.
[81] EHRM 12 januari 2016 (*Szabó & Vissy/Hongarije*), r.o. 56.
[82] EHRM 12 januari 2016 (*Szabó & Vissy/Hongarije*), r.o. 56, EHRM 4 december 2015 (*Roman Zakharov/Rusland*), r.o. 231.

121. Uit de Staatsburgse rechtspraak valt bovendien geen aanwijzing te halen dat de standaarden uit Weber *niet* zouden gelden in het geval van de vergaring van ruwe gegevens in bulk in het kader van internationale samenwerking.

122. In het arrest *Kennedy* wekt het EHRM de indruk dat juist het feit dat in die zaak geen sprake was van ongerichte grootschalige interceptie (maar van gerichte interceptie) mede ten grondslag ligt aan het oordeel dat de Britse waarborgen voldoende zijn.

> *The Court recalls its conclusion in Liberty and Others, cited above, § 65, that the authorities' discretion to capture and listen to captured material was very wide. However, that case, unlike the present case, involved external communications, in respect of which data were captured indiscriminately. Contrary to the practice under the Interception of Communications Act 1985 concerning external communications, interception warrants for internal communications under RIPA relate to one person or one set of premises only (cf. Liberty and Others, cited above, § 64), thereby limiting the scope of the authorities' discretion to intercept and listen to private communications. Moreover, any captured data which are not necessary for any of the authorised purposes must be destroyed.* [83]

123. En in *M.M./ UK*, waarin het ging om de opslag van gegevens in politieregisters, stelt het EHRM:

> *The greater the scope of the recording system, and thus the greater the amount and sensitivity of data held and available for disclosure, the more important the content of the safeguards to be applied at the various crucial stages in the subsequent processing of the data.*[84]

124. Dit wijst dus niet op een ontwikkeling dat voor grootschalige ongerichte interceptie minder hoge standaarden of minder waarborgen zouden moeten gelden, maar juist op het tegendeel.[85] Bij grootschalige, ongerichte interceptie gelden eerder hogere standaarden dan lagere. Hetzelfde geldt wanneer gegevens automatisch worden verwerkt.

> *The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes.*[86]

Bulkdata

125. Dat sprake is van de uitwisseling van grote hoeveelheden (ruwe) gegevens in bulk – ofwel grote hoeveelheden – die nog niet op relevantie zijn beoordeeld, zoals de rechtbank overweegt (r.o. 5.31), is dus juist een omstandigheid die noopt tot strengere waarborgen. Onjuist is ook de

[83] EHRM 18 mei 2010 (*Kennedy/UK*), r.o. 160 en 162.
[84] EHRM 13 november 2012 (*M.M/UK*), r.o. 200.
[85] Zie ook Mr. dr. J.P. Loof, mr. dr. J. Uzman, prof. mr. T. Barkhuysen, prof. mr. A.C. Buyse, prof. mr. J.H. Gerards, prof. dr. R.A. Lawson, *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, augustus 2015, p. 17, 40.
[86] EHRM 4 december 2008 (*S en Marper/UK*),r.o. 103, EHRM 18 april 2013 (*M. K./Frankrijk*), r.o.35. Zie ook HvJEU 8 april 2014, zaken C-293/12 en C-594/12 (*Digital Rights Ireland*), r.o. 55 en HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*), r.o. 91.

suggestie van de rechtbank aan het slot van r.o. 5.31 en 5.33, dat de inbreuk op de persoonlijke levenssfeer minder groot is als het de uitwisseling van bulkdata betreft, omdat de gegevens nog niet op relevantie zijn beoordeeld en "ten tijde van de ontvangst niet bekend is wat de aard van de gegevens is en op welk(e) individu(en) deze gegevens betrekking hebben".

126. Door aldus te oordelen heeft de rechtbank miskend dat het ongerichte en grootschalige karakter van de gegevensverzameling- en uitwisseling de inbreuk juist ernstiger maakt. Er zullen per definitie gegevens tussen zitten van onschuldige en onverdachte mensen, waardoor de beperking van het recht op privacy niet binnen de grenzen van het strikt noodzakelijke blijft.[87] Bij gerichte interceptie, daarentegen, is het bepalen van de noodzaak en proportionaliteit makkelijker.[88] Om die reden gaat de door de rechtbank gemaakte vergelijking met *Uzun/Duitsland*, waarin het ging om het verzamelen van GPS-data van een *concrete* verdachte, ook niet op.

127. Dat het uitwisselen van niet geëvalueerde bulkgegevens gevoelig is vanuit het oogpunt van het recht op privacy, overweegt ook de CTIVD in haar reactie op het concept wetsvoorstel tot wijziging van de Wiv:

> *De verstrekking van deze [ongeëvalueerde] gegevens is gevoelig vanuit het oogpunt van de bescherming van de persoonlijke levenssfeer, omdat nog niet is vastgesteld of de gegevens relevant zijn in relatie tot de taakuitvoering van de AIVD of de MIVD. Per definitie bevinden zich onder deze gegevens ook de persoonsgegevens van personen die geen relevantie hebben voor de nationale veiligheid. Bovendien gaat het bij ongeëvalueerde gegevens vaak om grote hoeveelheden (bulk).*[89]
>
> *[H]et past in de structuur van het concept-wetsvoorstel om ministeriële toestemming te vereisten waar de verstrekking van gegevens aan buitenlandse diensten een hoger risico met zich meebrengt dan gebruikelijk (bijvoorbeeld het verstrekken van ongeëvalueerde gegevens).*[90]

128. Ook het HvJEU is duidelijk over het doorgeven en bewaren van grote aantallen gegevens betreffende een onbeperkt aantal personen:

> *Niet beperkt tot het strikt noodzakelijke is dan ook een regeling die algemeen toestaat dat alle persoonsgegevens van alle personen van wie de gegevens vanuit de Unie naar de Verenigde Staten worden doorgegeven, worden bewaard, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het nagestreefde doel en zonder dat wordt voorzien in een objectief criterium ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan voor specifieke doeleinden, die*

[87] HvJEU 8 april 2014, zaken C-293/12 en C-594/12 (*Digital Rights Ireland*), r.o. 58.
[88] Vgl. Mr. dr. J.P. Loof, mr. dr. J. Uzman, prof. mr. T. Barkhuysen, prof. mr. A.C. Buyse, prof. mr. J.H. Gerards, prof. dr. R.A. Lawson, *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, augustus 2015, p. 16.
[89] Reactie CTIVD op het concept-wetsvoorstel wet op inlichtingen- en veiligheidsdiensten 20XX, 26 augustus 2015, p. 52.
[90] Reactie CTIVD op het concept-wetsvoorstel wet op inlichtingen- en veiligheidsdiensten 20XX, 26 augustus 2015, p. 54.

> *strikt beperkt zijn en als rechtvaardiging kunnen dienen voor de inmenging als gevolg van zowel de toegang tot als het gebruik van deze gegevens.*[91]

129. De ongerichte verzameling- en uitwisseling van bulkdata (zijnde zowel metadata als inhoud, r.o. 5.31) kan een sterk *chilling effect* hebben, want kan bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden, hetgeen van invloed kan zijn op de wijze waarop zij hun vrijheid van meningsuiting uitoefenen.[92] Dat raakt de wezenlijke inhoud van het recht op privacy, zo overweegt het HvJEU in *Digital Rights Ierland* en *Schrems*.

> *De bewaring van de gegevens met het oog op de eventuele raadpleging ervan door de bevoegde nationale autoriteiten, zoals bedoeld in richtlijn 2006/24, raakt rechtstreeks en specifiek het privéleven en dus de door artikel 7 van het Handvest gewaarborgde rechten. Een dergelijke bewaring van gegevens valt bovendien onder artikel 8 van dit Handvest omdat het gaat om een verwerking van persoonsgegevens in de zin van dit artikel.*[93]

> *Meer bepaald moet een regeling op grond waarvan de autoriteiten veralgemeend toegang kunnen krijgen tot de inhoud van elektronische communicatie worden beschouwd als een aantasting van de wezenlijke inhoud van het grondrecht op eerbiediging van het privéleven zoals door artikel 7 van het Handvest gewaarborgd.*[94]

130. Volledigheidshalve zij opgemerkt dat ook het door de rechtbank gemaakte onderscheid tussen metadata en inhoud (r.o. 5.31) niet tot een andere conclusie leidt. In de eerste plaats omdat, zoals de rechtbank zelf ook vaststelt, het zowel gaat om (bulk)gegevens die betrekking hebben op metadata als op de inhoud. In de tweede plaatst omdat metadata niet meer is wat het in de jaren ’80, ten tijde van de *Malone*-uitspraak, was. Uit metadata kunnen tegenwoordig, mede gelet op de technologische ontwikkelingen en mogelijkheden, zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren.[95] Dat vindt niet alleen het HvJEU, maar ook het EHRM.

> *The Court would add that the possibility occurring on the side of Governments to acquire a detailed profile (see the CDT’s submissions on this in paragraph 49 above) of the most intimate aspects of citizens’ lives may result in particularly invasive interferences with private life. Reference is made in this context to the views expressed by the Court of Justice of the European Union and the European Parliament (see paragraphs 23 and 25 above).*[96]

---

[91] HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*), ro. 93.
[92] HvJEU 8 april 2014, zaken C-293/12 en C-594/12 (*Digital Rights Ireland*), r.o. 28 en 37.
[93] HvJEU 8 april 2014, zaken C-293/12 en C-594/12 (*Digital Rights Ireland*), r.o.29.
[94] HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*), ro.94.
[95] HvJEU 8 april 2014, zaken C-293/12 en C-594/12 (*Digital Rights Ireland*), r.o. 27.
[96] EHRM 12 januari 2015 (*Szabó & Vissy/Hongarije*), r.o. 70.

131. Ook het kabinet erkent dat met metadata een grote inbreuk op het recht op privacy met zich mee kan brengen en meent dat het van oudsher gemaakte onderscheid tussen inhoud en metadata aan "relativering" toe.

> *In het licht van de constatering, dat het van oudsher gemaakte onderscheid tussen metadata enerzijds en de inhoud van de telecommunicatie anderzijds bij de beantwoording van de vraag naar de mate van inbreuk op de in geding zijnde grondrechten onder invloed van de steeds grote wordende schaal waarop gegevens voor verwerking in aanmerking komen en de steeds verdergaande mogelijkheden tot verwerking van die gegevens aan relativering toe is, voorziet het wetsvoorstel ook dienaangaande in aanvullende waarborgen.*[97]

Onderscheid verzamelen/verwerken

132. Uit het bovenstaande volgt al dat het door de rechtbank gemaakte onderscheid tussen het verzamelen (intercepteren of onderscheppen) van gegevens en het verder verwerken daarvan, niet opgaat. Zowel het verzamelen van gegevens als het verder verwerken daarvan levert een beperking van artikel 8 EVRM op. Beide inbreuken moeten afzonderlijk "bij wet zijn voorzien" zoals vereist door artikel 8 lid 2 EVRM.[98]

133. De rechtbank lijkt te suggereren dat het verzamelen niet zo kwalijk is, als de daaropvolgende verwerking maar met waarborgen is omkleed. Daarmee miskent de rechtbank echter dat ook het verzamelen *an sich* een beperking oplevert. Een ernstige beperking bovendien, zo blijkt onder meer uit de Digital Rights-uitspraak van het HvJEU. Daarin oordeelt het HvJEU dat het loutere opslaan van gegevens al een ernstige beperking van het privéleven met zich meebrengt. De latere toegang is aan aanvullende beperking van grondrechten.[99]

134. Onjuist is eveneens de overweging van de rechtbank dat de vraag in hoeverre de uitwisseling van gegevens een inbreuk op de persoonlijke levenssfeer van het individu meebrengt, "met name afhankelijk is van er met die gegevens gebeurt" (r.o. 5.32). Dat dit niet relevant is, heeft het HvJEU bevestigd.

> *Voor de vaststelling van een inmenging in het fundamentele recht op eerbiediging van de persoonlijke levenssfeer is het van weinig belang of de gegevens betreffende het privéleven al dan niet gevoelig zijn en of de betrokkenen door die inmenging enig nadeel hebben ondervonden.*[100]

135. Door aldus te oordelen heeft de rechtbank miskend dat één van de grootste problemen van ongerichte surveillance het *chilling effect* is – het gegevens dat mensen zich anders gaan gedragen als ze weten dat ze worden gevolgd. Zo typen mensen na de Snowden-onthullingen

---

[97] Memorie van Toelichting bij het concept-wetsvoorstel Wet op de Inlichtingen- en veiligheidsdiensten 20XX (consultatieversie juni 2015), p. 64. Zie ook p. 77.
[98] Mr. dr. J.P. Loof, mr. dr. J. Uzman, prof. mr. T. Barkhuysen, prof. mr. A.C. Buyse, prof. mr. J.H. Gerards, prof. dr. R.A. Lawson, *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, augustus 2015, p. 10.
[99] HvJEU 8 april 2014, zaken C-293/12 en C-594/12 (*Digital Rights Ireland*), r.o. 34-35.
[100] HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*), r.o. 87 en HvJEU 8 april 2014, zaken C-293/12 en C-594/12 (*Digital Rights Ireland*), r.o. 33.

significant minder controversiële zoektermen op Google in.[101] Dit *chilling effect* doet zich al voor bij de verzameling van persoonsgegevens, niet bij slechts bij de verwerking daarvan.[102]

136. In r.o. 5.30 hecht de rechtbank er nog aan dat de buitenlandse diensten van wie de AVID en de MIVD gegevens ontvangen, deze gegevens verzamelen op basis van de hun toekomende (bijzondere) bevoegdheden. Voor zover de rechtbank hiermee bedoelt dat de *nationale* wettelijke grondslag in de Wiv op basis waarvan de diensten samenwerken met buitenlandse diensten en op basis waarvan zij gegevens ontvangen dus geen waarborgen meer hoeft te bevatten, is dat onjuist gezien al het voorgaande. Op die manier zou het nationale (en Europese) beschermingsniveau bovendien eenvoudigweg (kunnen) worden omzeild. In *Schrems* maakt het HvJEU daar korte metten mee.[103] Voor zover de rechtbank suggereert dat onze diensten mogen vertrouwen op de waarborgen die gelden voor de buitenlandse diensten, is dat eveneens onjuist. Verwezen zij ook naar de toelichting op Grief 4. Gelet op alle Snowden-onthullingen, is dat vertrouwen niet (langer) gerechtvaardigd. Dat concludeert ook de CTIVD al in 2014:

> *De Commissie constateert dat de AIVD en de MIVD in de onderzochte hechte samenwerkingsverbanden er in grote mate op vertrouwen dat de desbetreffende buitenlandse diensten mensenrechten respecteren en handelen binnen de eigen nationale regelgeving. De Commissie is van mening dat het in het licht van de onthullingen van de afgelopen periode gewenst is om na te gaan of dit vertrouwen nog steeds terecht is. […] […] De Commissie beveelt de ministers van BZK en van Defensie in dit verband tevens aan de samenwerkingsrelaties (ook in internationaal verband) te beoordelen op transparantie en de afwegingen die ten grondslag liggen aan de samenwerking nader te concretiseren.* (**productie 8, p. 31**).

<u>Art. 59 Wiv bevat in het geheel geen waarborgen</u>

137. Uit het voorgaande volgt dat de rechtbank ten onrechte heeft geoordeeld dat de minimum waarborgen zoals hierboven omschreven niet vereist zijn bij internationale samenwerking op het gebied van geheime surveillance.

138. De rechtbank beperkt zich tot de conclusie dat het ontvangen van bulkgegevens door de Nederlandse diensten “niet aan zulke strenge waarborgen hoeft te voldoen als eisers voor ogen hebben” (r.o. 5.33). De rechtbank heeft niet getoetst of artikel 59 Wiv *überhaupt* voorziet in waarborgen. De vraag of dit artikel “onder alle omstandigheden de toets der kritiek kan doorstaan” heeft de rechtbank nadrukkelijk in het midden gelaten (r.o. 5.28).

139. Die belangrijke vraag had de rechtbank niet onbeantwoord mogen laten. De vraag of artikel 59 Wiv voldoet aan de eisen van artikel 8 lid 2 EVRM betreft immers de eerste vraag die relevant is voor de beoordeling van de geoorloofdheid van de ongebreidelde en ongecontroleerde uitwisseling van gegeven waar eisers bezwaar tegen maken.

---

[101] A A. Marthews & C. Tucker, Government Surveillance and Internet Search Behavior, gepubliceerd via SSRN: http://ssrn.com/abstract=2412564.
[102] O. van Daalen, ‘Burgers tegen Plasterk: het Nederlandse staartje van de Snowden-saga’, *AA* april 2015, p. 287-293.
[103] HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*), r.o. 73.

140. Zelfs als we ervan uit zouden gaan, zoals de rechtbank overweegt, dat de minimumwaarborgen uit *Weber* en *Liberty* niet onverkort gelden bij de ontvangst en het gebruik van gegevens in het kader van de samenwerking, had zij nog steeds moeten onderzoeken of artikel 59 Wiv dan in ieder geval *toereikende en effectieve* waarborgen tegen willekeur bevat.

141. De rechtbank heeft in r.o. 5.26 en 5.36 geoordeeld dat de ontvangst van gegevens in bulk in ieder geval moet voldoen aan "de meer algemene beginselen van bescherming tegen een willekeurige inbreuk", inhoudende (i) dat er een wettelijke basis bestaat, (ii) die de reikwijdte van een inmenging (of de bevoegdheid hiertoe), (iii) de voorwaarden voor de uitoefening van de discretionaire bevoegdheid bepaalt (r.o. 5.26) en die (iv) toereikende en effectieve waarborgen biedt tegen een willekeurige inbreuk (r.o. 5.36).

142. Die toets heeft de rechtbank ten onrechte niet verricht, maar als we die norm toepassen op artikel 59 Wiv, is direct duidelijk dat het artikel daar niet aan voldoet.

143. Artikel 59 Wiv spreekt slechts van het "onderhouden van verbindingen" met buitenlandse diensten. Het artikel bevat geen enkele voorwaarde, geen enkele waarborg – laat staan een voorzienbare – met betrekking tot het *ontvangen* van gegevens door de AIVD en de MIVD afkomstig van buitenlandse diensten of over het opslaan daarvan. De wetsgeschiedenis bevat slechts criteria voor het wel of niet aangaan van een samenwerking, over de inhoudelijke samenwerking en de reikwijdte daarvan als zodanig wordt niks geregeld. Dat wordt door de Staat ook ruiterlijk erkend, waar zij stelt dat de uitwisseling van gegevens tussen de diensten nou eenmaal "zonder bronvermelding" plaatsvindt.

144. Hierboven hebben we gezien dat de wettelijke grondslag voor een bevoegdheid niet zodanig zijn geformuleerd dat zij een vrijwel onbeperkte discretionaire bevoegdheid toekennen. Dit is precies wat artikel 59 doet. Het artikel bevat een onbeperkte, ongelimiteerde en oncontroleerbare bevoegdheid om gegevens uit te wisselen. Het artikel bevat geen waarborgen en voorziet niet in een vorm van onafhankelijk toezicht. Dat is in strijd met artikel 8 lid 2 EVRM. Dat de Wiv om die reden onvoldoende waarborgen biedt, heeft het Hof Den Haag bevestigd.[104]

Grief 6 – Bulkdata

Ten onrechte heeft de rechtbank geoordeeld dat het in deze zaak gaat om de uitwisseling van verzamelingen ruwe gegevens in bulk, onder meer in r.o. 5.17, 5.18, 5.24, 5.28, 5.31, 5.33, 5.38 en 5.49.

Toelichting

145. De rechtbank neemt in het vonnis als uitgangspunt dat het in deze zaak gaat om de uitwisseling ruwe gegevens in bulk (r.o. 5.18, 5.31), door de rechtbank gedefinieerd als gegevens die zijn verkregen door de inzet van bijzondere bevoegdheden die nog niet op relevantie zijn beoordeeld. Volgens de rechtbank kan het daarbij gaan om zowel metagegevens (ook wel metadata of verkeersgegevens) als om de eigenlijke inhoudelijke communicatie.

[104] Hof Den Haag 27 oktober 2015, ECLI:NL:GHDHA:2015:2881.

146. Het is onduidelijk waar de rechtbank dit standpunt op baseert. De Staat laat immers niks los over de (aard van de) gegevens die de AIVD en MIVD ontvangen van buitenlandse diensten, noch over de bronnen daarvan. Daardoor weten we helemaal niet of het alleen maar gaat om de uitwisseling van gegevens in bulk die niet op relevantie is beoordeeld.

147. In eerste aanleg zijn eisers uitvoerig ingegaan op de verschillende programma's en technieken waar de NSA en GCHQ zich van bedienen om gegevens te verzamelen. Daaruit blijkt dat de NSA e-mails, sms-berichten, chatberichten, telefoongesprekken, foto's, webcambeelden en een heleboel metadata verzamelt. De NSA verzamelt veel en verzamelt alles.

148. Ten onrechte heeft de rechtbank de zaak beperkt tot de uitwisseling van grote hoeveelheden, nog niet beoordeelde of geselecteerde data, "bulkdata". Maar belangrijker nog: ten onrechte wekt de rechtbank door het vonnis de suggestie dat de inbreuk om die reden minder ernstig is dan wanneer het zou gaan om inhoudelijke, specifieke informatie, onder meer waar zij oordeelt dat minder strenge eisen gelden ten aanzien van de voorzienbaarheid als het de ruwe uitwisseling van bulkdata betreft (r.o. 5.31). Omdat "ten tijde van de ontvangst niet bekend is wat de aard van de gegevens is en op welk(e) individu(en) deze betrekking hebben", zouden minder strenge waarborgen nodig zijn.

149. Zoals hierboven, bij de bespreking van grief 5, al is besproken, is die conclusie onjuist. Ook het verzamelen en uitwisselen van ruwe gegevens in bulk levert een inbreuk op het recht op privacy op, een ernstige inbreuk bovendien.

150. Onjuist is ten slotte de overweging van de rechtbank, dat zelfs als de verzamelingen gegevens mogelijk mede betrekking hebben op de inhoud van telecommunicatie (of het strategisch monitoren) daarvan, de ernst van de inbreuk op het privéleven niet gelijk gesteld kan worden aan die in de zaken die hebben geleid tot de Weber- en Libery-uitspraken (r.o. 5.31). Het HvJEU heeft immers bepaald dat in dat in dat geval niet alleen sprake is van een beperking van het grondrecht, maar zelfs van een aantasting van de wezenlijke inhoud van het grondrecht op privacy.

> *Meer bepaald moet een regeling op grond waarvan de autoriteiten veralgemeend toegang kunnen krijgen tot de inhoud van elektronische communicatie worden beschouwd als een aantasting van de wezenlijke inhoud van het grondrecht op eerbiediging van het privéleven zoals door artikel 7 van het Handvest gewaarborgd (zie in die zin arrest Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punt 39).*[105]

Grief 7 – Onderscheid verzamelen en verwerken

Ten onrechte overweegt de rechtbank in r.o. 5.32:

> "*Verder moet blijkens de rechtspraak van het EHRM ten aanzien van de eisen die aan de voorzienbaarheid van de wetgeving worden gesteld, worden onderscheiden tussen nationale wetgeving betreffende het verzamelen (intercepteren of onderscheppen) van gegevens*

[105] HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*), r.o. 94.

enerzijds en het verwerken van gegevens anderzijds. De rechtbank verwijst naar de uitspraak van het EHRM van 25 september 2001, app. no. 44787/98 (P.G. and J.H. v. The United Kingdom), par. 46-48). Het verzamelen van gegevens moet, uit het oogpunt van de eisen die het EVRM aan de nationale wetgeving stelt, derhalve worden onderscheiden van andere handelingen die op grond van de Wiv 2002 onderdeel zijn van de verwerking van gegevens, zoals bijvoorbeeld het opslaan, ordenen, raadplegen en samenbrengen en het in onderling verband brengen van gegevens, alsmede het extern verstrekken van gegevens. In hoeverre de uitwisseling van gegevens een inbreuk op de persoonlijke levenssfeer van het individu meebrengt, is met name afhankelijk van wat er met die gegevens gebeurt."

151. Ten onrechte maakt de rechtbank hier, ten aanzien van de eisen die aan de voorzienbaarheid van wetgeving worden gesteld, een onderscheid tussen het verzamelen en het verder verwerken van data, althans wekt zij de suggestie dat het loutere verzamelen – of ontvangen – minder problematisch zou zijn. Verwezen zij naar hetgeen daarover hierboven, bij de bespreking van grief 5, is opgemerkt.

152. Onjuist is ook de overweging van de rechtbank dat de vraag of sprake is van een privacyinbreuk vooral afhankelijk is van wat er met de verzamelde gegevens gebeurt. Dit is volgens het HvJEU van weinig belang:

> *Voor de vaststelling van een inmenging in het grondrecht op eerbiediging van het privéleven van weinig belang of de gegevens betreffende het privéleven al dan niet gevoelig zijn en of de betrokkenen door die inmenging enig nadeel hebben ondervonden (arrest Digital Rights Ireland e.a., C 293/12 en C 594/12, EU:C:2014:238, punt 33 en aldaar aangehaalde rechtspraak).*[106]

Grief 8 - Modus operandi

Ten onrechte overweegt de rechtbank in r.o. 5.34 en r.o. 5.35, waar zij ingaat op de "modus operandi" van inlichtingen- en veiligheidsdiensten, dat artikel 8 EVRM niet noopt tot een "hek aan de grens" als eenmaal aan de criteria voor samenwerking is voldaan. Eveneens ten onrechte overweegt de rechtbank dat de omstandigheid dat niet kan worden uitgesloten dat de Nederlandse diensten op die manier gegevens verwerven die in het buitenland zijn verzameld op een wijze die niet in overeenstemming is met artikel 8 EVRM, daaraan geen afbreuk doet. Ten onrechte overweegt de rechtbank verder dat "eenieder" in Nederland verschillende wegen kan bewandelen om de ontvangst en het gebruik van gegevens door de diensten die afkomstig zijn van (bepaalde) buitenlandse diensten te redresseren, onder meer via de CTIVD, de nationale ombudsman of de burgerlijke rechter.

Toelichting

153. De betreffende overwegingen van de rechtbank zijn onjuist om meerdere redenen. In de eerste plaats, omdat de rechtbank, door aldus te oordelen, de Staat in wezen wel degelijk een "vrijbrief" verschaft voor het handelen van de diensten bij het ontvangen van gegevens van buitenlandse diensten. In de tweede plaats omdat het feit dat een buitenlandse dienst aan de criteria voor samenwerking voldoet, anders dan de rechtbank overweegt, onvoldoende garanties voor de bescherming van grondrechten biedt. Tot slot zijn er, anders dan de rechtbank

[106] HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*), r.o. 87.

overweegt, geen toereikende middelen om de illegale ontvangst van gegevens door de Nederlandse diensten te redresseren.

Modus operandi geen absoluut verschoningsrecht

154. De Staat beroept zich in deze procedure op de “modus operandi” van inlichtingen- en veiligheidsdiensten. In de samenwerking is het niet gebruikelijk om te delen hoe gegevens zijn verzameld, aldus de staat. De informatie-uitwisseling vindt doorgaans zonder bronvermelding plaats.

155. Eisers hebben aangevoerd dat de omstandigheid dat het uitwisselen van gegevens tussen de diensten doorgaans zonder bronvermelding plaatsvindt, geen rechtvaardiging vormt voor het gebruik van gegevens die onder de Wiv 2002 niet hadden mogen worden verkregen. De “modus operandi” biedt geen vrijbrief voor het handelen in strijd met artikel 8 EVRM en artikel 7 en 8 van het Handvest.

156. De rechtbank overweegt in dit verband dat die feitelijke praktijk, waarbij diensten elkaar niet plegen te informeren over hun bronnen, echter niet door de Staat kan worden genegeerd, “terwijl uit het oogpunt van nationale veiligheid niet van de Staat kan worden verwacht dat hij de samenwerking met buitenlandse diensten als gevolg van die praktijk ook dan verbreekt als deze diensten op zichzelf voldoen aan de eerder geschetste criteria voor samenwerking.”

157. Door aldus te overwegen erkent – en aanvaardt – de rechtbank dus dat de werkwijze van inlichtingendiensten zich aan de democratische controle onttrekt en ook dat onze diensten simpelweg niet geïnformeerd worden over de herkomst van data. Kennelijk biedt de *modus operandi* de Staat, anders dan de rechtbank in het slot van r.o. 5.35 overweegt, dus wel degelijk een absoluut verschoningsrecht.

158. Als maar aan de criteria voor samenwerking wordt voldaan, is alles geoorloofd, zo lijkt de rechtbank te overwegen.

159. Daarmee gaat de rechtbank voorbij aan het betoog van eisers (pleitnotities 108-119) dat het niet zo “zwart-wit” is. Er zijn talloze gradaties denkbaar waarin diensten elkaar in meer of mindere mate zouden kunnen informeren over de bron van bepaalde informatie. Het is niet alles onthullen of niks onthullen.

160. De vraag of mededelingen kunnen worden gedaan over bronnen en methoden, hangt immers ook in belangrijke mate af van het *type* bron of het *type* methode. Zo ligt het voor de hand dat de identiteit van een natuurlijke persoon die heeft gefungeerd als bron niet wordt onthuld. Dit zou de betreffende persoon immers kunnen blootstellen aan potentiële gevaren. Dergelijke overwegingen spelen niet of in minder mate ten aanzien van papieren bronnen, of gehanteerde methodieken. Niet in te zien valt waarom ook daarover nimmer mededelingen zouden mogen worden gedaan. Waarom zou de Staat de Amerikanen en Britten niet kunnen vragen om een globale omschrijving van de gehanteerde werkwijzen, temeer nu een groot deel van de surveillanceprogramma’s die deze diensten gebruiken niet langer geheim zijn?

161. Dat het geen alles of niets is, volgt ook uit de wetsgeschiedenis. Daarin staat te lezen dat er, al naar gelang de samenwerkingsrelatie die er bestaat met een buitenlandse dienst, over en weer best wel wat meer openheid kan worden gegeven.[107]

162. Anders dan de Staat heeft aangevoerd, bevat artikel 15 van de Wiv evenmin een absolute verplichting om bronnen en methodes geheim te houden. Lid 2 van dat artikel spreekt van het geheimhouding van *daarvoor in aanmerking komende* bronnen waaruit gegevens afkomstig zijn. Deze terminologie laat uitdrukkelijk ruimte voor een nadere afweging. Bovendien beoogt het artikel met name zogenaamde "*humint*", human intellegince ofwel menselijke bronnen, te beschermen. Dat zegt ook de CTIVD:

> *De praktijk van de samenwerking tussen diensten brengt bepaalde beperkingen met zich mee op het gebied van openheid over de herkomst van gedeelde gegevens. Dit is ook onderkend in de wetsgeschiedenis. Daar wordt overwogen dat het in het verkeer tussen diensten niet gebruikelijk is om actief te informeren naar dan wel de ander te informeren over de methoden die gehanteerd zijn om bepaalde informatie boven water te krijgen. Net als de AIVD en MIVD hechten buitenlandse diensten eraan om bronnen en modus operandi geheim te houden. Ten aanzien van menselijke bronnen is dit meestal een wettelijke plicht, net zoals dit voor de AIVD en de MIVD het geval is (artikel 15 Wiv 2002). Al naar gelang de aard van de samenwerkingsrelatie die bestaat met een buitenlandse dienst kan er op dit punt over en weer meer openheid worden gegeven […]* (**productie 8, p. 83**).

163. Er zijn natuurlijk situaties denkbaar waarin de Staat bepaalde (lopende) operaties of personen moet beschermen, maar dat ontslaat de Staat niet van haar verplichting om meer transparantie na te streven ter bescherming van fundamentele rechten. In gelijke zin schrijft het Europees Parlement in haar recente rapport dat:

> *[W]hereas the fact that a certain level of secrecy is conceded to intelligence services in order to avoid endangering ongoing operations, revealing modi operandi or putting at risk the lives of agents, such secrecy cannot override or exclude rules on democratic and judicial scrutiny and examination of their activities, as well as on transparency, notably in relation to the respect of fundamental rights and the rule of law, all of which are cornerstones in a democratic society (**productie 15, p. 19**).*

164. Aan deze argumenten van eisers heeft de rechtbank ten onrechte geen aandacht besteed.

165. Onjuist is ook de overweging cq. suggestie van de rechtbank dat, als eenmaal aan de criteria voor samenwerking wordt voldaan, artikel 8 EVRM niet noopt tot een heks aan de grens.

166. Voor zover dat standpunt ooit überhaupt al houdbaar zou zijn geweest, geldt dat na de onthullingen van de afgelopen jaren in ieder geval niet meer. Die onthullingen hebben duidelijk gemaakt dat de Amerikanen veel te ver gaan en dat – dus – extra waarborgen vereist zijn. Er moet periodiek worden nagegaan of die waarborgen aanwezig zijn. Zo niet, dan mogen er

[107] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 63.

simpelweg geen gegevens worden uitgewisseld met de Amerikanen, zo overweegt het HvJEU in *Schrems*.[108]

167. De Commissaris voor de Mensenrechten in de Raad van Europa benadrukt in dit verband dat toezichthouders ("overseers") inzage moeten hebben in de ontvangen gegevens om die kritisch te kunnen beoordelen:

> *Access to information arising from and pertaining to international intelligence co-operation merits special consideration. In view of the extensive international co-operation between security services (and the impact that such co-operation can have on human rights) it is essential that overseers are able to scrutinise information about such co-operation, including information that has been received from or sent to foreign bodies.*[109]

168. Ook de CTIVD benadrukt dat de samenwerking met buitenlandse diensten geen statisch geheel is, maar voortdurend voorwerp moet zijn van evaluatie en – zo nodig – herziening. In het eerdere toezichtsrapport concludeert de CTIVD met zoveel woorden dat de diensten na moeten gaan of het "vertrouwen" nog terecht is, wat concreet betekent dat zij zich nader dienen te informeren over de wettelijke bevoegdheden en technische mogelijkheden van buitenlandse diensten (**productie 8, p. 31**). Bovendien moeten de ministers de samenwerkingsrelaties beoordelen op transparanties en de afwegingen die ten grondslag liggen aan de samenwerking nader concretiseren, aldus de CTIVD.[110] In het meer recente rapport over de MIVD benadrukt de CTIVD nog eens dat het ontvangen van gegevens niet zonder meer geoorloofd is. De diensten moeten oog hebben voor de rechtmatigheid van de verkregen informatie en alert zijn op aanwijzingen.[111]

169. De Staat moet dus kritisch zijn over de handelwijze van zusterdiensten en mag niet langer een oogje dichtknijpen. Die gedachte ligt ook ten grondslag aan het wetsvoorstel tot wijziging van de Wiv, die een bepaling voor heroverweging van de aard en intensiteit van de samenwerking bevat. Opgemerkt zij overigens dat dit voorstel, ook volgens de CTIVD, nog steeds te weinig waarborgen biedt.

Mogelijkheden achteraf niet voldoende

170. Anders dan de rechtbank stelt (r.o. 5.35), zijn er ook niet "verschillende wegen" om de ontvangst en het gebruik van gegevens door de diensten te redresseren. De door de rechtbank genoemde wegen bieden ieder geval geen voldoende waarborg. Onafhankelijke toezicht is niet denkbaar indien het toezichthoudende orgaan niet op zijn minst de bevoegdheid heeft om het (direct of indirect) tappen van advocaten te voorkomen of te beëindigen, zo oordeelde het Hof Den Haag.[112]

---

[108] HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*), r.o. 76-77.
[109] Issue paper published by the Council of Europe Commissioner for Human Rights, *Democratic and effective oversight of national security services*, mei 2015, p. 64.
[110] Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD, 5 februari 2014, CTIVD nr. 38, p. 31.
[111] Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen en/of veiligheidsdiensten, 10 juni 2015, CTIVD nr. 22B, p. 32.
[112] Hof Den Haag 27 oktober 2015, ECLI:NL:GHDHA:2015:2881, r.o. 2.9.

171. Over een dergelijke bevoegdheid beschikt de CTIVD niet. De bevoegdheden van de CTIVD zijn namelijk ontoereikend:

> *De CTIVD heeft weliswaar een toezichthoudende taak en kan uit dien hoofde zelfstandig onderzoek instellen naar de wijze waarop de Wiv 2002 is uitgevoerd (artikel 78), maar dit kan slechts uitmonden in het uitbrengen van een toezichtsrapport aan de Minister (artikel 79). Daarnaast kan de CTIVD de Minister gevraagd en ongevraagd adviseren en heeft zij een adviserende rol bij de behandeling van klachten (artikel 64 lid 2). Enige rechtstreekse betrokkenheid bij het tappen van advocaten heeft de CITVD niet, zij heeft bijvoorbeeld ook niet de bevoegdheid het tappen van een advocaat te (doen) beëindigen. De omstandigheid dat binnen de diensten beleidsmatig zekere waarborgen in acht worden genomen bij het tappen van advocaten en het uitwerken van onderschept materiaal, doet hier niet aan af. Het gaat daarbij immers niet om een vorm van onafhankelijk toezicht*.[113]

172. Daarmee is de CTIVD, anders dan de rechtbank stelt, niet het onafhankelijke toezichtsorgaan dat bij uitstek geschikt is om over de geoorloofdheid van de ontvangst en het gebruik van gegevens door de diensten te oordelen. Ook de CTIVD zelf vindt overigens dat zij over onvoldoende bevoegdheden beschikt. Het voornaamste gebrek is dat de CTIVD geen bindend rechtmatigheidsoordeel toekomt. De toezichthouder mist "tanden".[114]

173. Ook klachtbehandeling door de ombudsman, zoals door de rechtbank voorgesteld, biedt geen voldoende waarborgen. Nog daargelaten dat de ombudsman slechts kan oordelen over het bestuurlijk handelen van de overheid en helemaal geen zicht heeft op de handelwijze van de AIVD en MIVD, heeft het EHRM reeds geoordeeld dat klachtbehandeling door de ombudsman onvoldoende is, omdat deze geen bevoegdheid heeft een bindend oordeel te geven en geen specifieke verantwoordelijkheid om onderzoek te doen naar heimelijke informatieverzameling- en opslagoperaties.[115]

174. De burgerlijke rechter biedt evenmin het onafhankelijke toezicht dat in situaties al deze is vereist. In het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten, wordt geconcludeerd dat het EHRM op zijn minst de eis stelt van bindend ex post rechtmatigheidstoezicht door een externe afhankelijke toezichthouder. Bovendien moet er een onafhankelijke toezichthouder zijn die bindende oordelen kan geven in klachtprocedures.[116]

175. Conclusie van het voorgaande is dat de rechtbank het *modus operandi*-verweer van de Staat niet had mogen honoreren.

---

[113] Hof Den Haag 27 oktober 2015, ECLI:NL:GHDHA:2015:2881, r.o. 2.8. Zie ook Rb. Den Haag 1 juli 2015, ECLI:NL:RBDHA:2015:7436, r.o. 4.11.
[114] Reactie CTIVD op het concept-wetsvoorstel wet op inlichtingen- en veiligheidsdiensten 20XX, 26 augustus 2015.
[115] EHRM 26 maart 1987 (*Leander/Zweden*), ro. 82, EHRM 6 juni 2006 (*Segerstedt-Wiberg/Zweden*).
[116] Mr. dr. J.P. Loof, mr. dr. J. Uzman, prof. mr. T. Barkhuysen, prof. mr. A.C. Buyse, prof. mr. J.H. Gerards, prof. dr. R.A. Lawson, *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, augustus 2015, p. II, 18.

Grief 9 – Algemeen
Ten onrechte overweegt de rechtbank in r.o. 5.37 als volgt:

> "*Gelet op dit alles is de enkele omstandigheid dat rekening moet worden gehouden met de mogelijkheid dat de diensten gegevens ontvangen en gebruiken die door de buitenlandse diensten zijn verzameld op een wijze die niet in overeenstemming is met artikel 8 EVRM, onvoldoende voor de conclusie dat, bij gebreke aan de door eisers gestelde waarborgen in de Wiv 2002, de ontvangst en het gebruik door de diensten van gegevens afkomstig van buitenlandse diensten die zijn vergaard met de inzet van bevoegdheden waarover de diensten zelf niet beschikken onder alle omstandigheden in strijd met artikel 8 EVRM is*."

Toelichting
176. Volgens de rechtbank moet ernstig rekening worden gehouden met mogelijkheid dat de AIVD en de MIVD via buitenlandse diensten de beschikking krijgen over gegevens die met ongeoorloofde middelen zijn verkregen. Dit komt neer op het "witwassen" van illegale data. De Staat krijgt toegang krijgt tot gegevens die zij zelf nooit had mogen vergaren. Op die manier wordt onze eigen Nederlandse wetgeving, en de waarborgen die daarin zijn vastgelegd, volledig ondermijnd.

177. Het feit dat rekening moet worden gehouden met die mogelijkheid, noopt juist tot het implementeren van waarborgen en/het nemen van (positieve) maatregelen door de Staat. Verwezen zij naar de toelichting op grief 2, 4, 5 en 8.

Grief 10 – Noodzakelijkheidsvereiste
Ten onrechte overweegt de rechtbank in r.o. 5.39 als volgt:

> *"Volgens eisers valt niet in te zien waarom het noodzakelijk is dat de diensten de beschikking krijgen over gegevens die de buitenlandse diensten verkregen hebben door een schending van grondrechten en deze gegevens gebruiken. De Staat moet volgens eisers aantonen waarom niet naar de herkomst van informatie kan worden geïnformeerd en waarom de samenwerking niet op een minder ingrijpende manier kan. Niet aan de orde is evenwel de vraag of het noodzakelijk is om gegevens te verkrijgen die in strijd met artikel 8 EVRM zijn verworven. Het gaat om een dringende maatschappelijke behoefte dat met buitenlandse diensten wordt samengewerkt en dat in dat verband verzamelingen gegevens in bulk worden uitgewisseld. Zoals de Staat ter zitting naar voren heeft gebracht, kan wel naar de herkomst van informatie worden geïnformeerd, maar zal daarop in de regel geen antwoord worden gegeven. Dat, als een partner eenmaal aan de voor samenwerking geldende criteria voldoet, de aard en inhoud van die samenwerking, op voorhand niet zijn beperkt, is ook gerechtvaardigd gelet op de risico's voor de nationale veiligheid die aan een andere benaderingswijze zouden kunnen zijn verbonden. Van de Staat kan niet worden gevergd dat hij de dringend noodzakelijke samenwerking met buitenlandse diensten, zoals die van de VS, op het spel zet louter op grond van onbekendheid met hun werkwijze en de kans dat de Nederlandse diensten informatie ontvangen die is vergaard op een in Nederland niet toegelaten wijze. Het zwaarwegende belang van de nationale veiligheid geeft hier de doorslag*."

178. Deze grief richt zich tegen de overwegingen van de rechtbank ten aanzien van het noodzakelijkheidsvereiste, het vereiste dat elke beperking van het recht op bescherming van de persoonlijke levenssfeer "noodzakelijk" moet zijn in een democratische samenleving in de zin van artikel 8 lid 2 EVRM.

179. De rechtbank oordeelt in bovengenoemde overweging dat (artikel 59 van de) Wiv ook deze toets doorstaat. Volgens de rechtbank gaat het niet om de vraag of het noodzakelijk is om gegevens te verkrijgen die in strijd met artikel 8 EVRM zijn verworven, maar om de dringende maatschappelijke behoefte dat de Nederlandse diensten samenwerken met buitenlandse diensten en in dat verband verzamelingen gegevens in bulk uitwisselen.

180. De door de rechtbank gehanteerde toets is onjuist. De rechtbank keert het noodzakelijkheidsvereiste om. Artikel 8 lid 2 EVRM luidt immers:

> *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.*

181. Reeds uit deze bewoordingen blijkt dat de rechtbank had moeten onderzoeken of de *beperking* van het recht op privacy – de inmenging – noodzakelijk is in democratische samenleving. Dat heeft de rechtbank echter niet gedaan. De rechtbank heeft, daarentegen, onderzocht of er sprake is van een legitiem doel en geconcludeerd dat dat het geval is. De nationale veiligheid is gebaat bij samenwerking, dus is de beperking geoorloofd, zo lijkt de redenering van de rechtbank waar zij overweegt dat "het zwaarwegende belang van de nationale veiligheid [hier] de doorslag geeft". De rechtbank heeft ten onrechte niet onderzocht of de maatregel ook proportioneel – evenredig – is.

182. Dát (trans-)internationale samenwerking tussen inlichten- en veiligheidsdiensten noodzakelijk is, staat niet ter discussie. Dat hebben eisers ook aangegeven. De vraag of dat enkel op deze manier kan, waarbij onze diensten blind gegevens ontvangen, zonder navraag te doen naar de bron of op een andere manier te verifiëren dat het wel om rechtmatig verkregen materiaal gaat, staat dat wel.

183. Had de rechtbank de juiste toets aangelegd, dan had de conclusie moeten luiden dat de beperking niet voldoet aan het noodzakelijkheidsvereiste.

184. Zoals de rechtbank zelf ook constateert, moet sprake zijn van een dringende maatschappelijke behoefte (een "*pressing social need*") die de inbreuk op het grondrecht rechtvaardigt. Dit begrip dient restrictief te worden geïnterpreteerd, zeker als het geheime bevoegdheden betreft.[117] Het "noodzakelijkheidsvereiste" brengt daarnaast, zo overweegt ook de rechtbank, een

[117] Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD, 5 februari 2014, CTIVD nr. 38, p. 50.

proportionaliteitstoets met zich mee: de beperking moet in een redelijke verhouding staan tot het doel dat hiermee wordt beoogd en mag dus niet verder gaan dan redelijkerwijs noodzakelijk is. In dit vereiste ligt een vereiste van subsidiariteit besloten: wanneer met een lichtere inbreukmakende maatregel kan worden volstaan, is de inmenging niet proportioneel.[118]

185. In zaken over beperkingen in het belang van de nationale veiligheid, is het noodzakelijkheidsvereiste nauw verweven met het voorzienbaarheidsvereiste. Lidstaten hebben een zekere beoordelingsruimte (een "*margin of appreciation*") bij het inzetten van middelen in het belang van de nationale veiligheid, mits er voldoende waarborgen tegen willekeur bestaan.[119]

186. In *Roman Zakharov* vat het EHRM het noodzakelijkheidsvereiste als volgt samen:

> *As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court has acknowledged that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society" (see Klass and Others, cited above, §§ 49, 50 and 59; Weber and Saravia, cited above, § 106; Kvasnica v. Slovakia, no. 72094/01, § 80, 9 June 2009; and Kennedy, cited above, §§ 153 and 154).*[120]

187. In de recente uitspraak *Szabó* geeft het EHRM aan dat het noodzakelijkheidsvereiste, gezien "the potential of cutting-edge surveillance technologies to invade citizen's privacy" , zelfs vereist dat een beperking *strikt* noodzakelijk is. Daarvan is sprake als een maatregel strikt noodzakelijk is voor het verkrijgen van vitale informatie in een concreet geval.

> *[G]iven the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy, the Court considers that the requirement "necessary in a democratic society" must be interpreted in this context as requiring "strict necessity" in two aspects. A measure of secret surveillance*

[118] Zie onder meer EHRM 2 oktober 2011 (*Hatton/UK*), r.o. 97.
[119] Zie ook Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD, 5 februari 2014, CTIVD nr. 38, p. 50-51.
[120] EHRM 4 december 2015 (*Roman Zakharov/Rusland*), r.o. 232.

> *can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal.*[121]

188. Ook het HvJEU heeft benadrukt dat uitzonderingen op de bescherming van persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt moeten noodzakelijke blijven.[122]

189. Artikel 59 van de Wiv en de daarin vervatte, algemene bevoegdheid van onze diensten om ongevraagd gegevens, afkomstig van buitenlandse diensten, te ontvangen en gebruiken, voldoet niet aan deze norm. De bewijslast ter zake van het noodzakelijkheidsvereiste rust op de Staat. Dat is ook bevestigd door de Hoge Raad in de context van artikel 10 EVRM:

> *Dit brengt mee dat, wanneer de Staat wordt aangesproken uit onrechtmatige daad wegens inbreuk op art. 10 EVRM, het in zodanig geval in beginsel aan de Staat is — die ook bij uitstek in de gelegenheid is duidelijk te maken dat in het voorliggende geval niet met minder vergaande maatregelen kon worden volstaan — gemotiveerd te stellen en zo nodig te bewijzen dat deze inbreuk noodzakelijk is, welke stelplicht en bewijslast mede omvat dat de huiszoeking of doorzoeking in overeenstemming met de eisen van proportionaliteit en subsidiariteit heeft plaatsgevonden.*[123]

190. De Staat moet aantonen waarom het noodzakelijk is dat onze diensten illegale data gebruiken. De Staat moet aantonen waarom de samenwerking niet op een minder ingrijpende manier kan. Dat heeft zij niet gedaan. De Staat stelt slechts dat het uitwisselen van gegevens tussen de diensten nu eenmaal "zonder bronvermelding" plaatsvindt.

191. Dat is echter niet voldoende om de strenge noodzakelijkheidsdrempel te halen, zeker niet nu we weten op wat voor schaal de Amerikanen en de Britten inbreuk maken op de persoonlijke levenssfeer en wat voor technische middelen zij daarvoor gebruiken. Verwezen zij ook naar de toelichting op grief 8.

192. Zelfs als de Staat in een *concreet* geval zou kunnen motiveren waarom het nodig is om gebruik te maken van ontvangen, mogelijk illegale informatie, omdat dit "vital intelligence in an individual operation" betreft, biedt haar dat nog geen vrijbrief om in zijn algemeenheid en doorlopend (bulk)data te ontvangen van buitenlandse diensten op deze manier, zoals zij thans doet.

193. De huidige manier van samenwerking kan eenvoudigweg niet op dezelfde voet worden voortgezet. Zeker gelet op alle onthullingen over de werkwijze van buitenlandse diensten,

---

[121] EHRM 12 januari 2016 (*Szabó & Vissy/Hongarije*), r.o. 73.
[122] HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*), r.o. 92, HvJEU 8 april 2014, zaken C-293/12 en C-594/12 (*Digital Rights Ireland*), r.o. 52.
[123] HR 2 september 2005, *RvdW* 2005, 94, ECLI:NL:HR:2005:AS6926, r.o. 3.3.3. N.B. artikel 8 lid 2 EVRM moet hetzelfde geïnterpreteerd worden als artikel 10 lid 2 EVRM, zie bijvoorbeeld EHRM 25 maart 1983 (*Silver and other/UK*), r.o. 85.

moeten er waarborgen worden ingebouwd. Het HvJEU benadrukt het belang van waarborgen, juist wanneer persoonsgegevens automatisch worden verwerkt en er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd.[124] De CTIVD is van mening dat het in het licht van de onthullingen van de afgelopen periode gewenst is om na te gaan of het vertrouwen in de buitenlandse organisatie nog steeds terecht is (**productie 8**). In haar laatste toezichtrapport schrijft zij verder dat "bij het ongevraagd ontvangen van gegevens door de MIVD de vraag of die gegevens door de buitenlandse dienst rechtmatig zijn verkregen een belangrijke rol toekomt". De MIVD dient daarbij "bijzonder alert te zijn op aanwijzingen die aanleiding geven te twijfelen aan de rechtmatigheid van de verwerving van de gegevens door de buitenlandse dienst".[125]

194. Ook de Commissie Dessens vindt dat "het wettelijk kader in artikel 59 heroverweging verdient en dat, mede in het licht van de recente discussies over de NSA, nader onderzocht moet worden of de Wiv voor de samenwerking met buitenlandse diensten voldoende rechtsstatelijke en democratische garanties bevat." (**productie 11, p. 119**).

195. Hieruit blijkt wel dat adequate en effectieve waarborgen in de huidige Wiv ontbreken ter zake van het ontvangen van inlichtingen van buitenlandse diensten, zowel ten aanzien van het ontvangen van informatie als het gebruik daarvan. Dit terwijl de jurisprudentie van het EHRM die waarborgen wel vereist. Verwezen zij naar de toelichting op grief 5.

Grief 11 – Heroverweging en aanpassing Wiv

Ten onrechte overweegt de rechtbank in r.o. 5.39 als volgt:

"*De Snowden-onthullingen en het rapport van de CTIVD van 5 februari 2014 zijn aanleiding voor de Staat om (conform de aanbeveling van het CTIVD) de samenwerkingsrelaties (ook in internationaal verband) te beoordelen op transparantie en om de afwegingen die daaraan ten grondslag liggen nader te concretiseren. In dat verband zal ook artikel 59 Wiv 2002 worden aangepast. De rechtbank acht deze omstandigheden niet van belang voor haar beoordeling. Heroverweging van de samenwerking en aanpassing van de regelgeving zeggen immers op zichzelf niets over de rechtmatigheid van die samenwerking en regelgeving tot nog toe. Hetzelfde geldt voor de aanbevelingen van de Committee on Civil Liberties, Justice and Home affairs. Het aandringen op de naleving van artikel 8 EVRM impliceert niet dat die bepaling niet nageleefd wordt.*"

Toelichting

196. Ten onrechte gaat het rechtbank hier voorbij aan de mening van gezaghebbende commissies en toezichthouders, waaruit duidelijk blijkt dat het huidige kader niet in overeenstemming is met artikel 8 EVRM. De kritiek die zowel de CTIVD als de Commissie Dessens hebben geuit, met name over de vraag wat wel en niet geregeld is in de huidige wet en of er voldoende waarborgen bestaan tegen misbruik, zegt natuurlijk wel degelijk iets over de vraag of het huidige kader de toets van artikel 8 EVRM doorstaat.

[124] HvJEU 6 oktober 2015, zaak C- 362/14 (*Schrems*), r.o. 93.
[125] Juridische Bijlage bij het toezichtrapport over de samenwerking van de MIVD met buitenlandse inlichtingen en/of veiligheidsdiensten, *Het kader voor samenwerking met buitenlandse diensten*, p. 20.

197. Hetzelfde geldt vanzelfsprekend voor de ingrijpende wetswijziging die de Wiv momenteel ondergaat. Uit het feit dat de regering zelf meent dat het samenwerkingskader aan heroverweging toe is en waarborgen ontbeert, blijkt immers ook dat het thans geldende artikel 59 niet voldoet.

198. In ieder geval kan aan deze belangrijke conclusies en ontwikkelingen niet zonder nadere toelichting worden voorbijgegaan, zoals de rechtbank heeft gedaan.

Grief 12 – Artikel 10 EVRM

Ten onrechte overweegt de rechtbank in r.o. 5.41 als volgt:

> "[…] *Nu eisers geen zelfstandige gronden hebben aangevoerd voor hun beroep op schending van artikel 10 EVRM en de door hen genoemde bepalingen in het IVBPR, faalt het beroep op schending van die bepalingen eveneens*."

Toelichting

199. Onjuist is dat eisers "geen zelfstandige gronden hebben aangevoerd voor een beroep op schending van artikel 10 EVRM". Eisers, waaronder zich ook (verenigingen voor) journalisten bevinden, hebben immers het recht op bronbescherming van journalisten aangevoerd als zelfstandige grond (Dv 9, 49, 67), net zoals zij het verschoningsrecht van strafrechtadvocaten hebben aangevoerd als zelfstandige grond (Dv. 8)

200. Die zelfstandige grondslagen rechtvaardigen op zichzelf dat de vorderingen worden toegewezen. Dit klemt temeer, nu ten aanzien van beide reeds is geoordeeld dat adequate waarborgen tegen misbruik in de Wiv ontbreken. In de zaak *Telegraaf/AIVD*[126] heeft het EHRM unaniem geoordeeld dat de inzet van bijzondere bevoegdheden door de AIVD tegen journalisten een schending oplevert van artikel 8 en 13 EVRM, omdat niet voorzien is in een onafhankelijke bindende toets voorafgaand aan de inzet van die bevoegdheden tegen journalisten. In het wetsvoorstel tot wijziging van de Wiv heeft dit geresulteerd in een voorgesteld artikellid dat voorziet in een rechterlijke toetsing door de rechtbank Den Haag voorafgaand aan de inzet van bijzondere bevoegdheden tegen journalisten.[127]

201. Het Hof Den Haag oordeelde recent dat de Wiv ook wat betreft het verschoningsrecht van (strafrecht)advocaten niet de toets van artikel 8 EVRM kan doorstaan. Ook op dat front moet worden voorzien in extra waarborgen, zoals een onafhankelijke (rechterlijke) toetsing. [128]

202. Dat de afluisterpraktijken van de Amerikanen en Britten niet alleen het recht op privacy, maar ook andere fundamentele rechten, waaronder het recht op vrijheid van meningsuiting (artikel 10 EVRM, artikel 11 Handvest), in gevaar brengen, wordt treffend verwoord in het rapport van Mr. Pieter Omtzigt van het Parilamentary Assembly van de Raad van Europa:

---

[126] EHRM 22 november 2012 (*Telegraaf/AIVD*).
[127] Memorie van Toelichting bij het concept-wetsvoorstel Wet op de Inlichtingen- en veiligheidsdiensten 20XX (consultatieversie juni 2015), p. 35.
[128] Hof Den Haag 27 oktober 2015, ECLI:NL:GHDHA:2015:2881.

> *4. The surveillance practices disclosed so far endanger fundamental human rights, including the rights to privacy (Article 8 European Convention on Human Rights (ECHR), freedom of information and expression (Article 10, ECHR), and the rights to a fair trial (Article 6, ECHR) and freedom of religion (Article 9) - especially when privileged communications of lawyers and religious ministers are intercepted and when digital evidence is manipulated. These rights are cornerstones of democracy. Their infringement without adequate judicial control also jeopardizes the rule of law.*

Grief 13 – Positieve verplichting

Ten onrechte overweegt de rechtbank in r.o. 5.43 als volgt:

> "*Een positieve verplichting voor de Staat om in het kader van de internationale samenwerking bij de buitenlandse diensten steeds navraag te doen naar de wijze van vergaring van gegevens en burgers in de gelegenheid te stellen om te verifiëren of op ongeoorloofde wijze informatie over hen is vergaard en indien dit het geval is deze gegevens te wissen, vloeit niet voort uit het recht op bescherming van de persoonlijke levenssfeer zoals in artikel 8 EVRM neergelegd. Uit hetgeen hiervoor is overwogen in verband met artikel 59 Wiv 2002, blijkt dat de Staat niet verplicht is om voorafgaand aan de ontvangst van gegevens te informeren naar de wijze waarop gegevens door een buitenlandse dienst zijn verzameld. Uit artikel 8 EVRM vloeit evenmin een algemene informatieverplichting of verplichting tot vernietiging van gegevens, zoals eisers voorstaan, voort. Blijkens de rechtspraak van het EHRM valt een weigering van de nationale autoriteiten om toegang te verschaffen tot bepaalde persoonsgegevens binnen het toepassingsbereik van artikel 8 EVRM (vgl. eerdergenoemde uitspraak van het EHRM in de zaak Leander v. Sweden, par. 48). Dit laat onverlet dat in artikel 8 EVRM geen algemeen recht op toegang tot (persoons)gegevens is neergelegd, maar dat aan de hand van de concrete omstandigheden van het geval moet worden beoordeeld of een recht op toegang bestaat (zie EHRM 7 juli 1989, app. no. 10454/83, Gaskin v. The United Kingdom, par. 37). Voorts kan uit artikel 8 EVRM in het geval van geheime surveillance geen absolute notificatieverplichting achteraf worden afgeleid, aangezien dat praktisch onuitvoerbaar zou zijn (zie EHRM 6 september 1978, app. no 5029/71 (Klass v. Germany), par. 58).*"

<u>Toelichting</u>

203. Ten onrechte overweegt de rechtbank dat op de Staat geen positieve verplichting rust om haar burgers te beschermen tegen de Amerikaanse en Britse afluisterpraktijken, door navraag te doen naar de wijze waarop door de Staat ontvangen gegevens door die diensten zijn vergaard, door deze zo nodig te vernietigen en door burgers daarover te informeren.

204. Door aldus te oordelen, autoriseert de rechtbank de Staat in wezen om passief toe te kijken hoe buitenlandse veiligheids- en inlichtingendiensten de mensenrechten schenden. Verwezen zij ook naar de toelichting op grief 8.

205. Juist in het kader van artikel 8 EVRM heeft het EHRM in haar rechtspraak talloze malen benadrukt dat dit recht niet alleen een negatieve verplichting voor de Staat bevat om zich van

inbreuken op de privacy te onthouden, maar ook een verplichting tot doen, een positieve verplichting.

> *The Court recalls that although the object of Article 8 (art. 8) is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life [...]. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves.*[129]

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

> *[...] The boundaries between the State's positive and negative obligations under Article 8 do not lend themselves to precise definition. The applicable principles are nonetheless similar. In particular, in both instances regard must be had to the fair balance to be struck between the competing interests.* [130]

207. De omvang van de afluisterpraktijken van buitenlandse diensten en de (maatschappelijke) belangen die op het spel staan, zijn dusdanig groot, dat de Staat niet langer stilzwijgend kan blijven toekijken. Dat vindt ook het Europees Parlement, dat lidstaten oproept om te voldoen aan hun positieve verplichting om de persoonlijke levenssfeer van hun burgers te beschermen, onder meer door te voorkomen dat het recht van een derde land de eigen wetgeving ondermijnt.

> *27. Calls on the Member States immediately to fulfil their positive obligation under the European Convention on Human Rights to protect their citizens from surveillance contrary to its requirements, including when the aim thereof is to safeguard national security, undertaken by third states or by their own intelligence services, and to ensure that the rule of law is not weakened as a result of extraterritorial application of a third country's law* (**productie 15, p. 25**)

208. In de Prakken d'Oliveira-zaak aarzelden de rechtbank en het Hof Den Haag niet om de Staat een positieve verplichting op te leggen. Dit omdat de omvang van de inzet van bijzondere bevoegdheden jegens advocaten en hun cliënten onvoldoende duidelijk was. Daarmee hield de Staat de mogelijkheid dat communicatie van en met verschoningsgerechtigden werd afgeluisterd nadrukkelijk open. De Staat was daarom gehouden om – ter nadere bescherming van het verschoningsrecht en op een effectieve verdediging en toegang tot het recht – maatregelen te nemen die onafhankelijke controle mogelijk maken op de uitoefening van de bijzondere bevoegdheden.[131]

[129] Zie onder meer EHRM 15 maart 2012 (*Aksu/Turkije*), EHRM 5 april 2005 (*Monory/ Romania and Hungary*).
[130] EHRM 4 december 2007 (*Dickson/ UK*).
[131] Rb. Den Haag 1 juli 2015, ECLI:NL:RBDHA:2015:7436, r.o. 4.15, bekrachtigd door het Hof.

209. Niet in te zien valt waarom een dergelijke verplichting niet zou gelden voor de bevoegdheid om samen te werken met buitenlandse diensten en daarmee gegevens uit te wisselen. Onder de huidige bevoegdheid houdt de Staat immers ook nadrukkelijk de mogelijkheid open dat op die manier illegale data wordt verkregen en witgewassen. De Snowden-onthullingen rechtvaardigen dat de Staat maatregelen neemt om dat tegen te gaan, en in ieder geval dat zij maatregelen neemt om het risico daarop zo veel mogelijk te verkleinen.

210. Die mening is ook de CTIVD toegedaan. De toezichthouder is van mening dat het ontvangen van gegevens door de Nederlandse diensten onrechtmatig is als het bij de Nederlandse diensten bekend is of bekend verondersteld mag worden dat deze gegevens door de buitenlandse dienst zijn verzameld op een manier die naar Nederlandse maatstaven een ongeoorloofde inbreuk op de persoonlijke levenssfeer oplevert (**productie 8, p. x**). In het meer recente toezichtsrapport over de MIVD overweegt de CTIVD dat diensten zich bij het gebruik van ontvangen gegevens moeten afvragen of dit geoorloofd is. Zij herhaalt in dit verband dat onze diensten zich moeten verdiepen in de wettelijke bevoegdheden en technische mogelijkheden van bondgenoten.[132]

211. Niet in te zien valt hoe dat in de praktijk op een andere manier kan worden vormgegeven dan door – in ieder geval tot op zekere hoogte – navraag te doen naar de bronnen en werkwijze van de buitenlandse dienst, anders dan de rechtbank overweegt (r.o. 5.43).

212. Dat sluit ook goed aan bij de (doorlopende) verplichting van de Staat om de samenwerking met buitenlandse diensten te evalueren en te heroverwegen, zoals uiteengezet in de CTIVD-rapporten, maar ook in de nieuwe Wiv. Een dergelijke positieve verplichting valt ook af te leiden uit de Schrems-uitspraak.

> *Ook staat het aan de Commissie, met het oog op het feit dat het door een derde land geboden beschermingsniveau aan ontwikkelingen onderhevig kan zijn, om […] periodiek na te gaan of de constatering dat het door het derde land in kwestie geboden beschermingsniveau passend is, nog steeds in feite en in rechte gerechtvaardigd is. Een dergelijk onderzoek dringt zich in elk geval op wanneer er aanwijzingen zijn die daarover twijfels doen ontstaan.*

213. Het HvJEU is in die uitspraak niet teruggedeinsd van vergaande consequenties op het moment dat blijkt dat een derde land niet meer voldoet. In dat geval kan de gegevensuitwisseling simpelweg niet op dezelfde voet worden doorgezet, aldus het HvJEU. Dat zou resulteren in een omzeiling van de Europese regels en dat is niet geoorloofd.

214. Dat uit artikel 8 EVRM geen *algemene* informatie- of notificatieverplichting voortvloeit en geen *algemene* verplichting tot vernietiging van gegevens, zoals de rechtbank overweegt, doet aan een en ander niet af. Het grote probleem zit hem immers in de fase daarvoor: het ontvangen van gegevens van buitenlandse diensten, zonder dat op enige manier wordt gewaarborgd dat gegevens waarover de Staat via buitenlandse diensten de beschikking krijgt op geoorloofde wijze zijn verkregen.

---

[132] Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen en/of veiligheidsdiensten, 10 juni 2015, CTIVD nr. 22B, p. 32. Zie ook Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD, 5 februari 2014, CTIVD nr. 38, p. 32.

Grief 14 – Handvest van de grondrechten van de EU
Ten onrechte heeft de rechtbank de handelwijze van de Staat niet separaat getoetst aan het Handvest.

Toelichting

215. De rechtbank heeft louter artikel 8 EVRM bij haar oordeel betrokken. Daarmee is de rechtbank voorbij gegaan aan de toetsing aan de artikelen 7, 8 en 11 van het Handvest, welke eisers ook ten grondslag hebben gelegd aan hun vorderingen. De gegevens die worden uitgewisseld worden beschermd op grond van artikel 8 van het Handvest, de surveillance is onder meer strijdig met artikel 7 van het Handvest, het afluisteren van advocaten is mede in strijd met artikel 11. Het Handvest stamt uit 2009, vormt primair Unierecht, en biedt meer bescherming dan het EVRM.

216. De toepasselijkheid van het Handvest kan niet omzeild worden door de handelwijze van de diensten het predicaat "staatsveiligheid" te geven. Er wordt op grote schaal inbreuk gepleegd op de persoonlijke levenssfeer die niets met de staatsveiligheid te maken heeft. Het HvJEU heeft in *Schrems* ook geen enkele moeite gehad het Handvest toe te passen op handelingen van de Amerikaanse dienst NSA.

217. Voor zover uw hof aarzelt over de toepasselijkheid van het Handvest, geven eisers uw hof eerbiedig in overweging hier prejudiciële vragen over te stellen.

CONCLUSIE

Dat het het Gerechtshof behage het vonnis van de rechtbank Den Haag op 23 juli 2014 onder zaaknummer/rolnummer C/09/455237/ HA ZA 13-1325 gewezen tussen appellanten als eisers en geïntimeerde als gedaagde te vernietigen en, opnieuw rechtdoende, de vorderingen van appellanten alsnog toe te wijzen, met veroordeling van geïntimeerden in de kosten van beide instanties, uitvoerbaar bij voorraad.

Behandelend advocaat

Deze zaak wordt behandeld door
Mr. Chr.A. Alberdingk Thijm en mr. C.F.M. de Vries
bureau Brandeis
Apollolaan 151 1077 AR Amsterdam The Netherlands
T: 020 7606 505 / F: 020 7 606 555
info@bureaubrandeis.com / bureaubrandeis.com