Het Schrems/Facebook-arrest en de gevolgen voor internationale doorgifte

Mr. O.L. van Daalen*

De overdracht van persoonsgegevens naar de Verenigde Staten vond tot voor kort plaats op basis van de zogenoemde Safe Harbour-beschikking.[1] Het Hof van Justitie heeft die beschikking een paar maanden geleden ongeldig verklaard.[2] Dit is een uitspraak met serieuze gevolgen voor de doorgifte van persoonsgegevens buiten Europa en voor privacybescherming in het algemeen. Wat is de redenering van het Hof van Justitie en wat zijn de gevolgen?

HvJ 6 oktober 2015, zaak C-362/14, Facebook/Schrems, ECLI:EU:C:2015:650

De aanloop naar de ongeldigverklaring van de Safe Harbour-beschikking

In de Richtlijn bescherming persoonsgegevens (Rbp) is een streng regime voor de doorgifte van persoonsgegevens buiten de Europese Unie of de Europese Economische Ruimte opgenomen.[3] Doorgifte is in beginsel alleen toegestaan naar een land dat een 'passend beschermingsniveau' voor persoonsgegevens waarborgt (art. 25 lid 1 Rbp). Met andere woorden: de regels in dat land moeten persoonsgegevens voldoende beschermen.

De Europese Commissie en de lidstaten kunnen bepalen dat een land géén passend beschermingsniveau biedt (art. 25 lid 4 Rbp) – en in dat geval moeten lidstaten maatregelen nemen om doorgifte naar dat land te voorkomen. Maar de Commissie kan ook bepalen dat het beschermingsniveau van een land wél passend is – eventueel na onderhandelingen tot aanpassing van de regelgeving in dat land – en in dat geval moeten lidstaten zich ook voegen naar *dat* besluit (art. 25 lid 6 Rbp).

De Safe Harbour-beschikking van de Europese Commissie is zo'n besluit: daarin heeft de Europese Commissie bepaald onder welke omstandigheden het beschermingsniveau in de Verenigde Staten passend – en doorgifte naar dat land dus toegestaan – is. De beschikking is de uitkomst van onderhandelingen tussen de Europese Commissie en de Verenigde Staten. Die onderhandelingen waren er in eerste instantie op gericht om het beschermingsniveau van de Verenigde Staten op het Europese niveau te krijgen. De regels in de VS zijn namelijk minder streng: waar Europa privacyregelgeving kent die voor alle sectoren geldt, zijn die regels in Amerika maar in beperkte mate sectoroverstijgend en waar in Europa de regels ook gaan over proportionaliteit van inbreukmakende maatregelen, gaan ze in de Verenigde Staten vooral over transparantie en naleving daarvan.

Het is de Europese Commissie echter niet gelukt om de privacyregelgeving van de VS aan te passen. De uiteindelijke Safe Harbour-beschikking verschilt daarom in één belangrijk opzicht van de andere zogenoemde '*adequacy*' beschikkingen. In de beschikking is namelijk niet besloten dat een *land* (de Verenigde Staten) een passend beschermingsniveau heeft, maar dat bepaalde *Amerikaanse bedrijven* onder voorwaarden worden geacht een voldoende beschermingsniveau te bieden. De Europese Commissie heeft hiervoor waarschijnlijk gekozen omdat de Verenigde Staten hun regels niet wilden aanpassen, terwijl de Europese Commissie de economische belangen zo groot achtte dat ze graag een deal wilde sluiten.

Dit betekende dat als een Amerikaans bedrijf zich hield aan de 'Safe Harbour Privacy Principles' – een lijst met privacybeginselen – doorgifte vanuit de EU naar dat bedrijf was toegestaan.

Bedrijven konden makkelijk profiteren van de Safe Harbour-regeling. Het was een systeem van zelfcertificering: vanaf het moment dat een bedrijf aan het Amerikaanse Department of Commerce had aangegeven dat

* Mr. O.L. (Ot) van Daalen is onderzoeker bij het Instituut voor Informatierecht van de Universiteit van Amsterdam en advocaat te Amsterdam.

1. Beschikking 2000/520/EG, *PbEG* 2000, L 215/7.
2. HvJ 6 oktober 2015, zaak C-362/14, *Facebook/Schrems*, ECLI:EU:C:2015:650.
3. Richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *PbEG* 1995, L 238.

doi: 10.5553/NtER/138241202016022003002

het zich aan deze beginselen zou houden mocht overdracht plaatsvinden. Er vond voorafgaand aan de certificering dus geen toets plaats óf een bedrijf zich ook aan de Principles hield. De Principles lieten bovendien veel ruimte aan bedrijven om de naleving zelf vorm te geven. Ze waren minder dan 800 woorden lang (terwijl de Rbp meer dan 12.000 woorden lang is) en lieten ruimte voor interpretatie. Bovendien – belangrijk voor het arrest dat hier besproken wordt – mocht de toepasselijkheid van deze beginselen beperkt worden op grond van de nationale veiligheid van de Verenigde Staten.

Sinds het aannemen van de beschikking in 2000 hebben duizenden bedrijven zich als Safe Harbour-compliant aangemeld. Dit waren vaak bedrijven met vestigingen in Amerika en Europa die de overdracht van gegevens tussen die vestigingen mogelijk wilden maken. De lijst van deze bedrijven staat nog steeds online, en daarop staan typische internetbedrijven zoals Microsoft en Facebook maar ook meer 'fysieke' bedrijven zoals Tesla (dat gegevens over het gebruik van zijn auto's naar Amerika wil kunnen overdragen).

Tegelijkertijd concludeerde de Commissie al vrij snel dat het systeem niet goed werkte. In een Working Paper uit 2002 schrijft de Commissie: 'A substantial number of organisations that have self-certified adherence to the Safe Harbour do not seem to be observing the expected degree of transparency as regards their overall commitment or as regards the contents of their privacy policies.'[4] In een daaropvolgende evaluatie concludeert de Commissie opnieuw dat een deel van de Safe Harbour-gecertificeerde bedrijven niet voldoet aan alle Safe Harbour-vereisten.[5] Toch was de handhaving van Safe Harbour door de Federal Trade Commission (FTC) zeer beperkt: de FTC heeft haar eerste handhavingszaken pas in 2009 gestart en de handhaving sindsdien werd volgens de Commissie onvoldoende geacht.[6]

Maar wat de discussie echt op scherp zette, is dat uit de documenten van Edward Snowden blijkt dat de Amerikaanse afluisterdienst, de National Security Agency (NSA), op grote schaal toegang heeft tot gegevens bij Amerikaanse bedrijven. Zo blijkt de NSA via een van de afluisterprogramma's, PRISM, rechtstreekse toegang te krijgen tot de grootste Amerikaanse internetbedrijven, zoals Yahoo, Microsoft en Facebook. Dit zijn bedrijven die op basis van de Safe Harbour-beschikking allemaal gegevens van Europese burgers importeerden naar de VS – en deze daarmee dus makkelijker toegankelijk maakten voor de NSA.

Dat was voor de Europese Commissie zelf al een reden om een onderzoek te starten naar de herziening van de Safe Harbour-afspraken. Zij publiceerde in 2013 een mededeling over het herstel van het vertrouwen in gegevensstromen tussen de EU en de VS.[7] Daarin concludeert ze dat Safe Harbour-certified bedrijven de beginselen niet altijd naleven, en dat de NSA via de Safe Harbour-beschikking toegang kreeg tot gegevens van Europeanen. Tegelijkertijd vindt ze het te ver gaan om de beschikking in te trekken, want dat zou de handelsrelaties tussen de EU en de VS te veel schaden. Ze startte daarom onderhandelingen met de VS over aanpassingen van de Safe Harbour-beschikking.

Ondertussen lag niet alleen de Safe Harbour-beschikking onder vuur: ook het Handvest van de Grondrechten van de Europese Unie is aangenomen. Het Handvest kent een aparte bepaling over de bescherming van persoonsgegevens (art. 8). In lid 3 staat dat een onafhankelijke autoriteit erop toeziet dat deze regels worden nageleefd.

De onthulling van PRISM was voor een Oostenrijker, Max Schrems, de aanleiding om zich te richten op de Safe Harbour-beschikking. Het Handvest – en de voorgeschreven onafhankelijkheid van toezichthouders – bood daarbij een mooi juridisch aanknopingspunt. Schrems richtte zich op Facebook: hij is een gebruiker van Facebook, en Facebook is een van de bedrijven die meedeed aan het PRISM-programma. Facebook heeft een Ierse vestiging, en gegevens van Europese gebruikers van Facebook werden op basis van de Safe Harbour-regeling naar de Amerikaanse moedermaatschappij, Facebook Inc., doorgegeven (en daarmee toegankelijk gemaakt voor de NSA).

Schrems verzocht de Ierse privacytoezichthouder daarom de overdracht van zijn persoonsgegevens door Facebook Ierland naar Facebook Inc. te verbieden. Hij stelde dat de Safe Harbour niet meer 'safe' was – want het was nu bewezen dat de NSA op grote schaal toegang krijgt tot gegevens – en dat de Ierse toezichthouder, mede in het licht van het Handvest, bevoegd was om doorgifte te verbieden. De Ierse toezichthouder wees de klacht echter af: Schrems heeft niet bewezen dat de NSA toegang tot zijn gegevens had gekregen, en bovendien is de toezichthouder gebonden aan de Safe Harbour-beschikking van de Commissie (en daaruit zou al volgen dat Facebook Inc. een passend beschermingsniveau waarborgt). Deze afwijzing vocht Schrems aan bij het Ierse High Court, en dat stelde vervolgens prejudiciële vragen aan het Hof van Justitie. Die leidden tot dit spraakmakende arrest.

De uitspraak van het Hof van Justitie

De twee prejudiciële vragen die het Ierse High Court aan het Hof van Justitie heeft voorgelegd gaan in de kern over de vraag of de Ierse toezichthouder de Com-

4. Zie Commission Staff Working Paper on Safe Harbour, 13 februari 2002, SEC(2002) 196, te vinden op <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/sec-2002-196_en.pdf>.
5. Zie Commission Staff Working Document on evaluation of Safe Harbour, 20 oktober 2004, SEC(2004) 1323, te vinden op <https://web.archive.org/web/20060724173657/http://www.ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2004-1323_en.pdf>.
6. Zie Communication from the Commission on the Functioning of the Safe Harbour, COM(2013)847 final, par. 5.1, te vinden op <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013DC0847>.
7. Zie COM(213)846 final, te vinden op: <http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf>.

doi: 10.5553/NtER/138241202016022003002

missiebeschikking naast zich neer had mogen leggen. Het Hof van Justitie stelt allereerst vast dat een Commissiebeschikking alleen door het Hof van Justitie ongeldig verklaard kan worden (punt 52). De Ierse toezichthouder kan dus niet zelf de Safe Harbour-beschikking ongeldig verklaren. Maar het *toezicht* op internationale doorgifte – zelfs in het kader van zo'n beschikking – is volgens het Hof van Justitie niet aan de bevoegdheidssfeer van die toezichthouder onttrokken (punt 54). Sterker nog: de toezichthouder is 'verplicht om in volledige onafhankelijkheid' op verzoek van een betrokkene onderzoek te doen naar de doorgifte van persoonsgegevens (punt 57).

Juist omdat de toezichthouder niet de bevoegdheid heeft om een Commissiebeschikking zelf ongeldig te verklaren – enkel om een specifieke doorgifte te verbieden – is de toezichthouder verplicht om een verzoek dat *erop neerkomt* dat die beschikking ongeldig is met de 'nodige voortvarendheid en zorgvuldigheid' te onderzoeken (punt 63). Bij een afwijzing kan de klager dan namelijk in beroep gaan, zodat de beschikking uiteindelijk – net zoals bij de zaak van Schrems – uitkomt bij het Hof van Justitie, dat wel een oordeel mag vellen over de geldigheid (punt 64). Sterker nog: als de toezichthouder zelf, dus op eigen initiatief, concludeert dat een beschikking ongeldig is, dan moeten er ook voor hem rechtswegen openstaan om dit via een prejudiciële vraag bij het Hof van Justitie te laten aankomen (punt 65).

Na deze introductie neemt het Hof van Justitie ook de volgende stap: het onderzoekt de geldigheid van de Safe Harbour-beschikking – wat overigens opmerkelijk is, omdat de prejudiciële vragen voldoende ruimte lieten om die vraag niet te beantwoorden.

Het stelt allereerst vast dat het vereiste van een passend beschermingsniveau tot doel heeft om het 'hoge niveau' van bescherming in Europa voort te zetten als gegevens naar een derde land worden doorgegeven (punt 73). Dat komt erop neer dat het 'importerende' land een beschermingsniveau van 'de grondrechten en fundamentele vrijheden biedt dat in grote lijnen overeenkomt' met het niveau binnen de Europese Unie ('*essentially equivalent*') (punt 73) – ook al zijn de middelen om die bescherming te waarborgen anders (punt 74).

Dat betekent dat de Europese Commissie bij de beoordeling van 'passendheid' onderzoek moet doen naar (1) het recht in dat land en (2) de praktijk waarmee de naleving wordt gewaarborgd. Zij moet hierbij alle omstandigheden die op de doorgifte van invloed zijn in acht nemen (punt 75). Dat moet zij niet alleen doen op het moment dat zij voor de eerste keer de passendheid beoordeelt, maar ook periodiek daarna, zeker wanneer er aanwijzingen zijn die daarover twijfels doen ontstaan – denk aan de Snowden-onthullingen (punt 76). Die periodieke toetsing moet – niet verrassend – ook rekening houden met gebeurtenissen die na de goedkeuring hebben plaatsgevonden (punt 77).

Het Hof van Justitie zegt ook iets over de manier waarop *het Hof zelf* zo'n passendheidsbesluit van de Commissie moet toetsen: het Hof van Justitie moet hier strikt toezicht op uitoefenen, gelet op de grote privacy-impact van zo een besluit (punt 78).

Vervolgens past het Hof van Justitie deze uitgangspunten toe op de Safe Harbour-beschikking van de Commissie. Die analyse pakt niet goed uit. Amerikaanse overheidsinstanties zijn niet tot naleving van de Safe Harbour-beginselen verplicht (punt 82), en er is niet vastgelegd welke maatregelen de VS precies moeten nemen om een passend beschermingsniveau te waarborgen (punt 83).

Belangrijker is nog dat in een bijlage bij de Safe Harbour-beschikking is bepaald dat de Safe Harbour-beginselen beperkt kunnen worden voor zover nodig voor nationale veiligheid, algemeen belang en rechtshandhaving (punt 84). Ook heeft de Commissie niets opgemerkt over (1) of de Amerikaanse overheid aan bepaalde proportionaliteitseisen is gebonden bij de opvraging van gegevens bij Safe Harbour-bedrijven op grond van deze beperking (punt 88) en (2) of er rechtsbescherming wordt geboden (punten 89 en 90).

Dat gebrek aan – in één woord – proportionaliteit nekt de Safe Harbour-beschikking. Daarbij schenkt het Hof van Justitie aandacht aan de *opslag* en aan de *toegang* tot gegevens. Ten aanzien van de *opslag* merkt het Hof van Justitie op dat 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'

(niet verrassend) niet proportioneel is (punt 93). Deze overweging doet denken aan de overwegingen van het Hof van Justitie in *Digital Rights Ireland* over de opslag van telecomgegevens onder de Bewaarplichtrichtlijn, waar het Hof van Justitie ook bezwaar had tegen het onbeperkte karakter.[8]

Ten aanzien van de *toegang* tot die gegevens merkt het Hof van Justitie op dat – zoals het eerder in *Digital Rights Ireland* deed – het 'veralgemeend' toegang kunnen krijgen tot de *inhoud* van elektronische communicatie de wezenlijke inhoud van het recht op privacy (art. 7 Handvest) aantast.[9] Dat de betrokkene niet de mogelijkheid heeft om inzage, rectificatie of verwijdering van gegevens van persoonsgegevens te eisen is bovendien in strijd met het wezen van het recht op een effectieve voorziening in rechte (art. 47 Handvest).

8. Zie HvJ 8 april 2014, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238, punten 58-59.
9. *Digital Rights Ireland*, punt 39 e.v.

doi: 10.5553/NtER/138241202016022003002

Na al deze uitgebreide overwegingen over de privacy-impact van de Safe Harbour-beschikking is de conclusie bijna een anticlimax: het Hof van Justitie constateert namelijk dat de Commissie in de Safe Harbour-beschikking niet heeft vermeld dat de Verenigde Staten op basis van hun wetgeving 'waarborgen bieden' voor een passend beschermingsniveau (punt 97). Alleen daarom – en zonder dat de beschikking inhoudelijk hoeft te worden beoordeeld – is artikel 1 (waarin is bepaald dat de Safe Harbour Principles passende bescherming bieden) ongeldig (punt 98). De vraag dringt zich overigens op waarom het Hof van Justitie zich daarvoor zo uitgebreid bekommert over de inhoudelijke eisen die volgen uit het Handvest. Ook artikel 3 van de beschikking, waarin toezichthouders worden beperkt in hun uit de Rbp en het Handvest voortvloeiende bevoegdheid om doorgifte op te schorten, is ongeldig (punten 102-104). Omdat die twee artikelen zo sterk verbonden zijn met de rest van de artikelen, verklaart het Hof van Justitie de hele Safe Harbour-beschikking ongeldig.

Dat is een vergaande conclusie. Het past tegelijkertijd wel in een lijn van zaken over privacy (waaronder die over de Bewaarplichtrichtlijn en die over het *right to be forgotten*) waarin het Hof van Justitie niet bang is om stevige conclusies te trekken – zelfs als die conclusies vergaande juridische, politieke en maatschappelijke gevolgen hebben.[10] Wat zijn die gevolgen?

De gevolgen van het arrest

Laten we beginnen met de juridische gevolgen. Een belangrijk juridisch gevolg is dat de onafhankelijkheid van de toezichthouders op het gebied van gegevensbescherming hiermee wordt bevestigd. Toezichthouders moeten de bevoegdheid hebben om zelf onderzoek te doen naar internationale doorgifte. Daarmee hangt samen dat toezichthouders voortvarend klachten moeten behandelen. De Artikel 29 Werkgroep – het samenwerkingsverband van Europese toezichthouders op het gebied van gegevensbescherming – waarschuwde dan ook dat de toezichthouders zouden gaan handhaven als niet eind januari 2016 een nieuw akkoord over Safe Harbour in zicht was.[11]

Bovendien moeten toezichthouders de juridische mogelijkheid hebben om zelf een rechtszaak te beginnen waarmee ze de geldigheid van een passendheidsbeschikking aan het Hof van Justitie kunnen voorleggen. Dat kan de Nederlandse privacytoezichthouder, de Autoriteit Persoonsgegevens (AP), op dit moment niet, omdat ze een ZBO zonder rechtspersoonlijkheid is.[12] Ik verwacht dat de AP die bevoegdheid voorlopig ook niet gaat krijgen, in ieder geval niet vóór inwerkingtreding van de Algemene verordening gegevensbescherming (de vervanging van de Rbp, ook wel bekend als de Privacyverordening) over twee jaar.

Dit arrest is ook juridisch belangrijk omdat het de toezichthouders meer onder druk zet. Toezichthouders moeten klachten die de geldigheid van passendheidsbeschikkingen aan de orde stellen namelijk voortvarend oppakken. Dat heeft waarschijnlijk tot gevolg dat toezichthouders in de verschillende lidstaten zich actiever zullen opstellen, ook al zullen sommige dat schoorvoetend doen (de Ierse toezichthouder wekte sterk de indruk deze zaak oorspronkelijk niet te willen behandelen).[13]

Als we kijken naar de meer inhoudelijke eisen maakt het arrest een gekke draai: eerst besteedt het Hof van Justitie veel aandacht aan de toets die moet worden toegepast op massasurveillance, en vervolgens verklaart het de beschikking ongeldig vanwege een soort 'vormfout' (namelijk dat de Commissie had verzuimd om uitdrukkelijk te vermelden dat de VS passende waarborgen bieden). Die draai is moeilijk te plaatsen, maar het betekent in ieder geval dat het Hof van Justitie het niet wilde laten bij een bespreking van de motiveringsplicht van de Europese Commissie.

Sterker nog: het Hof van Justitie grijpt deze gelegenheid aan om verder uit te leggen hoe de privacybepalingen in het Handvest moeten worden uitgelegd. Dit is ook relevant voor nationale wetgeving die de verwerking door de overheid van persoonsgegevens op grote schaal mogelijk maakt. Een voorbeeld hiervan is het voorstel voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten, dat de ongerichte interceptie van kabelgebonden communicatie zou introduceren.[14] De regering zal opnieuw – na de stevige uitspraak in *Digital Rights Ireland* – moeten onderzoeken of deze plannen in overeenstemming zijn met de rechten die in het Handvest worden beschermd.

Het is tot slot juridisch belangrijk omdat een van de meest gebruikte instrumenten voor internationale gegevensoverdracht naar de Verenigde Staten hiermee ongeldig is verklaard. Dat heeft mogelijk gevolgen ten aanzien van doorgiften die al *hebben* plaatsgevonden. Volgens de regering moet het ervoor worden gehouden dat ook die doorgiften onrechtmatig zijn, omdat het Hof van Justitie in het midden laat in hoeverre de ongeldigverklaring terugwerkt.[15] Daar staat tegenover dat het arrest waar de regering zich op baseert voor deze conclusie ongeldigverklaring met terugwerkende kracht

10. *Digital Rights Ireland* en HvJ 13 mei 2014, zaak C-131/12 , *Costeja Gonzales (Google Spain SL en Google Inc. tegen Agencia Española de Protección de Datos (AEPD) en Mario Costeja González)*, ECLI:EU:C:2014:317.
11. Zie Artikel 29 Werkgroep, Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems/Data Protection Commissioner case (C-362-14), te vinden op: <http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf>.
12. Zie de pagina over mandaatregelingen van de AP, <https://autoriteitpersoonsgegevens.nl/nl/over-het-cbp/bestuur-en-beleid/mandaatregelingen>.
13. Zie de processtukken in de *Schrems*-zaak, te vinden op de website van Europe v. Facebook: <http://europe-v-facebook.org/EN/Complaints/complaints.html>.
14. Zie Consultatie Voorstel van Wet op de inlichtingen- en veiligheidsdiensten 20.., te vinden op: <www.internetconsultatie.nl/wiv>.
15. Zie *Kamerstukken II* 2015/16, 32 317, nr. 363, p. 7.

doi: 10.5553/NtER/138241202016022003002

juist als uitzondering benoemt.[16] Hoe het ook zij: deze twijfel over de effecten van de ongeldigverklaring leidt op zijn minst tot rechtsonzekerheid, al zal die rechtsonzekerheid vooral afhangen van de bereidheid van private initiatieven om via constructies zoals claimstichtingen eventuele schade te verhalen op Facebook.

Wat wel zeker is, is dat het Safe Harbour-framework geen basis biedt voor de doorgifte naar de VS in de toekomst. De Hamburgse privacytoezichthouder is het doorgifteverbod zelfs gaan handhaven tegen drie bedrijven.[17] Omdat veel bedrijven ernstig onthand zouden zijn als ze de doorgifte moeten stopzetten, hebben zij ondertussen gekozen voor het makkelijkste alternatief met het minste risico: *standard contractual clauses*. Deze door de Europese Commissie opgestelde modelbepalingen zijn bedoeld om de internationale doorgifte van een bedrijf in de EU naar een bedrijf daarbuiten met waarborgen te omkleden. Eén waarborg die zo'n contract echter niet kan bieden, is dat de gegevens – als ze eenmaal in bijvoorbeeld de VS zijn – vervolgens door geheime diensten van dat land worden opgevraagd.

Daarmee zijn ook die modelbepalingen kwetsbaar. Ten eerste is in de beschikkingen waarmee de modelbepalingen zijn goedgekeurd, opgenomen dat een toezichthouder een doorgifte mag opschorten als deze 'in aanzienlijke mate afbreuk dreigt te doen aan de waarborgen die de betrokkene een passende bescherming bieden'.[18] Dit is vooral problematisch voor doorgifte naar bedrijven waarvan vaststaat dat deze toegang geven aan de NSA tot persoonsgegevens (bijvoorbeeld via PRISM).[19] Maar de privacytoezichthouder van Schleswig-Holstein suggereert zelfs dat iedere doorgifte op basis van deze modelbepalingen ongeldig zou kunnen zijn.[20] Dit is een omstreden positie.[21] Ondertussen is de AP – in ieder geval naar buiten toe – minder voortvarend: sinds de ongeldigverklaring heeft de AP op haar website verwezen naar de communicatie van de Artikel 29 Werkgroep hierover – die stelde dat de Europese Commissie aan zet was.[22]

De uitkomst van de onderhandelingen over een opvolger van de Safe Harbour-beschikking is daarom des te belangrijker. De eerste stappen zijn inmiddels bekend: de Europese Commissie heeft onlangs een nieuwe conceptpassendheidsbeschikking gepubliceerd over deze opvolger, het Privacy Shield.[23] Het voert te ver om de beschikking hier uitgebreid te bespreken. Een aantal punten is echter opvallend. Ten eerste is het mechanisme waarmee de Europese Commissie toezeggingen van de Verenigde Staten hoopt te krijgen opmerkelijk: via een aantal brieven van Amerikaanse hooggeplaatsten, en niet door nieuwe wetten aan te nemen. Het is ook opvallend dat de VS in die brieven aangeven dat zij nog steeds gegevens van Europese burgers in bulk kunnen onderscheppen.[24] Toezeggingen van de VS zijn wat dat betreft niet geruststellend: 'It is important to emphasize that any bulk collection activities regarding Internet communications that the U.S. Intelligence Community performs through signal intelligences operate on a small proportion of the Internet.'[25] Ook zouden de VS weliswaar een nieuwe ombudspersoon in het leven roepen die Europeanen kan helpen bij het verkrijgen van informatie over Amerikaanse surveillance, maar het is de vraag of die ombudspersoon voldoende bevoegdheden krijgt om zijn taak goed uit te oefenen.

Schrems heeft in een relatief uitgebreide analyse dan ook al een aantal redenen genoemd waarom het Privacy Shield onvoldoende bescherming zou bieden – en de passendheidsbeschikking de toets van het Hof van Justitie dus niet zou doorstaan.[26] Die is inmiddels opgevolgd door een grondige beoordeling van de Artikel 29 Werkgroep, en zij deelt een aantal van de bovengenoemde zorgen.[27] Hoewel het er netjes staat, concludeert de Artikel 29 Werkgroep tussen de regels door dat dat het huidige concept niet voldoet aan de 'essentially equivalent'-toets. Er moet volgens de Artikel 29 Werkgroep nog heel wat veranderen aan de passendheidsbeschikking, wil deze de toets wel doorstaan.

16. Zie M. Jansen, 'Minister persisteert: ook historische uitwisselingen persoonsgegevens met V.S. dankzij Schrems-arrest onrechtmatig', 1 februari 2016, te vinden op <http://dirkzwagerieit.nl/2016/02/01/minister-persisteert-ook-historische-uitwisselingen-persoonsgegevens-met-vs-dankzij-schremsarrest-onrechtmatig/>.
17. Zie A. Gruber, 'Schonfrist vorbei: Datenschützer will Safe-Harbor-Sünder zu Bußgeldern verdonnern', Spiegel Online 24 februari 2016, te vinden op: <www.spiegel.de/netzwelt/netzpolitik/safe-harbor-hamburgs-datenschuetzer-droht-firmen-mit-bussgeld-a-1079019.html>.
18. Zie art. 4 lid 1 sub a Beschikking 2001/497/EG van de Commissie van 15 juni 2001 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen krachtens Richtlijn 95/46/EG, *PbEG* 2001, L 181/19 en art. 4 lid 1 sub a Beschikking 2010/87 van 5 februari 2010 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens aan in derde landen gevestigde verwerkers krachtens Richtlijn 95/46/EG, *PbEG* 2010, L 39/5.
19. Zie ook Schrems' commentaar op de uitspraak: <http://europe-v-facebook.org/EN/Complaints/PRISM/Response/response.html>.
20. Zie ULD Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015, C-362/14, par. 5, te vinden op <https://www.datenschutzzentrum.de/artikel/981-ULD-Position-Paper-on-the-Judgment-of-the-Court-of-Justice-of-the-European-Union-of-6-October-2015,-C-36214.html>.
21. Zie bijvoorbeeld L. Moerel, 'An assessment of the impact of the Schrems judgement on the data transfer grounds available under EU data protection law for data transfers to the U.S.', te vinden op <www.mofo.com/~/media/Files/ClientAlert/2016/02/160201OpinionimpactoftheEC.pdf>.
22. Zie Cbp, 'Privacytoezichthouders: EC aan zet na uitspraak Safe Harbour', 16 oktober 2015, te vinden op <https://autoriteitpersoonsgegevens.nl/nl/nieuws/privacytoezichthouders-ec-aan-zet-na-uitspraak-safe-harbour>.
23. Zie Draft decision on the adequacy of the protection provided by the EU-U.S. Privacy Shield, te vinden op <http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf>.
24. Zie Annex VI bij draft EU-US Privacy Shield, waarin staat beschreven dat Amerikaanse surveillancewetgeving 'directs that signal intelligence collection be as tailored as feasible and that signals intelligence collected in bulk can only be used for specific enumerated purposes' en 'signals intelligence collected in bulk can only be used for six specific purposes'.
25. Zie de vorige noot.
26. Zie M. Schrems, "First summary of potential issues and problems on Privacy Shield", te vinden op: http://mschrems.com/PS_Feedback.pdf.
27. Zie "Privacytoezichthouders kritisch over privacyschild", 13 april 2016, te vinden op: https://autoriteitpersoonsgegevens.nl/nl/nieuws/privacytoezichthouders-kritisch-over-privacyschild en Opinion 01 /2016 on the EU – U.S. Privacy Shield draft adequacy decision, WP 238, te vinden op: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

doi: 10.5553/NtER/138241202016022003002

De twijfels over het antwoord op de vraag of het Privacy Shield een 'essentially equivalent' beschermingsniveau biedt, worden trouwens alleen maar pregnanter op het moment dat de Privacyverordening in werking treedt.[28] De Privacyverordening moet immers de Richtlijn bescherming persoonsgegevens vervangen. De verwachting is dat de verordening in de komende maanden zal worden gepubliceerd in het publicatieblad, waarna deze na twee jaar in werking treedt: ergens in 2018 dus. Tegelijkertijd vereist ook deze verordening dat het land waarnaar gegevens worden geëxporteerd een passend beschermingsniveau waarborgt – de toets is dus dezelfde gebleven als onder de Richtlijn bescherming persoonsgegevens, dus de bescherming moet gelet op de uitspraak van het Hof van Justitie 'essentially equivalent' zijn. De verordening is op punten echter strenger dan de huidige richtlijn. Het is te hopen dat de Artikel 29 Werkgroep die omstandigheid ook meeneemt in haar analyse.

Ondertussen is het de vraag of de gemiddelde internetgebruiker hiervan iets gaat merken. Dat lijkt me sterk. Toezichthouders en bedrijven zullen het waarschijnlijk niet zo ver laten komen dat persoonsgegevens niet meer naar de VS doorgegeven mogen worden. Daardoor zou een belangrijk deel van veelgebruikte internetdiensten niet goed meer werken. En het is voor toezichthouders onwenselijk als privacy wordt geassocieerd met het blokkeren van populaire internetdiensten.

Maar bovendien had Max Schrems zo'n uitkomst waarschijnlijk niet voor ogen. Zijn doel was om het systeem van internationale doorgifte en Amerikaanse surveillance aan de kaak te stellen. Of die Amerikaanse surveillance serieus zal worden ingeperkt door deze rechtszaak valt te bezien, maar de discussie wordt gevoerd. Daarover kan hij tevreden zijn.

28. Zie het artikel 'Europese gegevensbescherming: van richtlijn naar verordening' van Peter Schelven en Ivo Schelven over de Privacyverordening elders in dit *NTER*-nummer.

doi: 10.5553/NtER/138241202016022003002