Hof van Justitie EU (Grote Kamer)
6 oktober 2015, zaak C-362/14
(Skouris, (president), Lenaerts, Tizzano, Silva de Lapuerta, von Danwitz, Rodin, Jürimäe, Rosas, Juhász, Borg Barthet, Malenovský, Šváby, Berger, Biltgen en Lycourgos)
Noot: M.E. Koning

Eerbiediging privéleven en communicatie. Bescherming persoonsgegevens. Veiligehavenregeling. Veiligehavenbeginselen. Safe Harbor. Passend beschermingsniveau. Extraterritoriale werking Handvest. Doorgifte derde landen.

[art. 1, 25, 26, 31 lid 2 95/46/EG; art. 7, 8, 47 Hv; 2000/520/EG; section 702 FISA; art. 33-35 Wiv 20XX]

De klager Schrems heeft een Facebookaccount en heeft hiervoor een contract getekend met Facebook Ireland, dat (een gedeelte van) de persoonsgegevens doorgeeft aan Facebook Inc. in de Verenigde Staten. Facebook gebruikt hier de zogenaamde Veiligehavenregeling voor, dat is gebaseerd op een uit het jaar 2000 stammend toereikendheidsoordeel van de Europese Commissie (EC) dat het algemene verbod op doorgifte van persoonsgegevens naar derde landen buiten de Europese Unie (EU) opheft voor verantwoordelijken die gegevens doorgeven aan organisaties in de VS die middels zelfcertificering aan een aantal privacybeginselen voldoen. De Veiligehavenbeschikking bood een "veronderstelling van een passend beschermingsniveau". Schrems vroeg de Ierse toezichthouder om Facebook Ireland te verbieden om zijn persoonsgegevens naar de Verenigde Staten door te geven omdat het geldende recht en de praktijk in dat land geen waarborgen bieden voor afdoende bescherming. De toezichthouder meende niet in de positie te zijn om de klacht van Schrems te onderzoeken. De zaak belandde bij de Ierse High Court, dat zich in een prejudiciële verwijzing afvraagt of en in hoeverre – in het licht van art. 7, 8 en 47 van het Handvest van de Grondrechten van de Europese Unie (Hv) – zo'n toereikendheidsoordeel de toezichthouder in de weg staat bij het onderzoeken van een privacyklacht over de gegevensdoorgifte naar een gegevensverwerker in het derde land, wanneer de klager aanvoert dat het geldende recht en de praktijk in dat land geen waarborgen voor een passend beschermingsniveau bieden. Het HvJ EU geeft hier een tweeledig antwoord op. In de eerste plaats damde de Veiligehavenbeschikking de bevoegdheid van de toezichthouder in door een hoge drempel voor interventie op te werpen. Hiermee ging de EC haar boekje te buiten omdat zij enkel ex art. 25 lid 6 95/46/EG bevoegd is tot het vaststellen van een beschikking over het passend beschermingsniveau in een derde land en niet om de bevoegdheden van de nationale toezichthouder in te perken. In de tweede plaats legt het HvJ EU uit dat de toezichthouder in het land van de gegevensexporteur bevoegd is toezicht te houden op de doorgifte. Het feit dat enkel het HvJ EU de bevoegdheid heeft om de ongeldigheid van een handeling van de Unie vast te stellen, doet niet af aan de onderzoeksbevoegdheid van de toezichthouders. Ook wanneer een klacht bij een toezichthouder gericht is op de legitimiteit van de regels, en niet op de legitimiteit van de toepassing van de regels, moet de toezichthouder de mogelijkheid hebben om in rechte op te kunnen treden. In dat geval moet de toezichthouder een klacht die zij gegrond acht aan de nationale rechter kunnen voorleggen, zodat die laatste, wanneer hij de twijfel ten aanzien van de legitimiteit deelt, de vraag naar de geldigheid van dat toereikendheidsoordeel prejudicieel kan verwijzen, een en ander in het licht van art. 47 Hv. Het HvJ EU toetst vervolgens de Veiligehavenbeschikking aan art. 7, 8 en 47 Hv en legt uit dat een toereikendheidsoordeel regelmatig moet worden beoordeeld. Zelfcertificering, zoals in de Veiligehavenregeling, is in beginsel niet in strijd met de grondrechten, maar de waarborgen voor een passend beschermingsniveau moeten blijken uit de nationale wetgeving

of internationale verbintenissen van het derde land, ex art. 25 lid 6 95/46/EG. Een passend beschermingsniveau moet in grote lijnen overeenkomen met het niveau dat binnen de Unie wordt gewaarborgd op grond van 95/46/EG en het Handvest. Het gegevensbeschermingsrecht heeft dus een extraterritoriale reikwijdte. Vanwege de ruime en zware inbreuk van eventuele wetsontduiking via gegevensverwerking in een derde land dat geen passend beschermingsniveau biedt, toetst het HvJ EU strikt. De Veiligehavenbeschikking zwijgt over de verdere gegevensverwerking van persoonsgegevens van EU-burgers door de Amerikaanse overheid en onderstreept dat de privacybeginselen genegeerd kunnen worden indien de Amerikaanse wet een tegenstrijdige plicht aan de gegevensverwerker oplegt. Daarnaast is het onduidelijk of de regeling beperkt is tot het strikt noodzakelijke omdat de autoriteiten algemene toegang kunnen krijgen tot de inhoud van elektronische communicatie. Dit beschouwt het HvJ EU als een aantasting van de wezenlijke inhoud van het grondrecht op eerbiediging van het privéleven ex art. 7 Hv. Ook wordt het ontbreken van een adequate rechtsbescherming voor EU-burgers in de VS gezien als een aantasting van de wezenlijke inhoud van het grondrecht op een effectieve voorziening in rechte ex art. 47 Hv. Effectieve rechterlijke toetsing bestaat om de naleving van de bepalingen van Unierecht te verzekeren, en is inherent aan het bestaan van een rechtsstaat, aldus het HvJ EU. Op grond van deze bezwaren en de beperking die de Veiligehavenbeschikking de toezichthouder oplegde, acht het HvJ EU beschikking 2000/520 ongeldig.

Maximillian Schrems
tegen
Data Protection Commissioner

[Uitspraak]

[Annotatie]

1. Binnen twee weken nadat de Advocaat Generaal (AG) zijn Conclusie had gegeven oordeelde de Grote Kamer van het Hof van Justitie van de EU (HvJ EU) in deze zeer actuele *Schrems*-zaak. De zaak kwam op naar aanleiding van de Snowden-onthullingen over de verregaande sleepnetsurveillance gericht op buitenlanders door onder meer de National Security Agency (NSA) in samenwerking met Amerikaanse sociale-mediabedrijven. De klacht richtte zich op de doorgifte van persoonsgegevens naar de Verenigde Staten van Amerika (VS) door Facebook Europe, gevestigd in Ierland. Deze annotatie richt zich op het tweede deel van het arrest, dat overigens leest als een spannend boek, waarin het HvJ EU ingaat op de geldigheid van de Veiligehavenbeschikking in het licht van art. 7,8 en 47 Hv. Alvorens op de lange- en kortetermijneffecten van de uitkomst van het arrest in te gaan, sta ik kort stil bij de algemene structuur van de bepalingen voor doorgifte van persoonsgegeven naar derde landen zoals neergelegd in de Gegevensbeschermingsrichtlijn 95/46/EG en de specifieke eigenschappen van de Veiligehavenbeschikking.
2. De twintig jaar oude gegevensbeschermingsrichtlijn is van toepassing op de persoonsgegevensverwerking in publieke en private sector. De richtlijn dient een tweeledig doel: enerzijds het bieden van een gelijkwaardig hoog beschermingsniveau van grondrechten in alle EU Lidstaten en anderzijds het vrije verkeer van gegevens in de EU bevorderen. De meest prominente beperking van de reikwijdte is de uitsluiting van gegevensverwerking in de politie- en inlichtingensector ex art. 3 lid 2 95/46/EG.
3. De regels omtrent doorgifte van gegevens naar derde – buiten de Unie gevestigde – landen moeten worden gezien als een verlengstuk van het hoogwaardig beschermingsniveau van de Richtlijn dat een extraterritoriaal effect aan de fundamentele rechten en vrijheden van de EU

geeft. Gegevensstromen naar derde landen zijn in beginsel alleen toegestaan indien dat land een passend beschermingsniveau waarborgt ex art. 25 lid 1 95/46/EG. Dit niveau moet voortvloeien uit de nationale wetgeving en/of internationale verplichtingen omtrent privacybescherming van het derde land en wordt beoordeeld op basis van alle omstandigheden die van invloed zijn op de situatie, ex art. 25 lid 2 95/46/EG. Momenteel heeft de EC elf beslissingen genomen ex art. 25 lid 6 juncto 31 lid 2 95/46/EG omtrent het passend beschermingsniveau, waarvan er nu dus eentje is vernietigd door het HvJ EU.

4. Op twee manieren kan van de passend beschermingsniveauregeling worden afgeweken. In de eerste plaats kunnen middels contractuele bepalingen voldoende en passende privacywaarborgen worden ingesteld door de voor de verwerking verantwoordelijke ex art. 26 lid 2 95/46/EG. De EC heeft vier sets modelcontractbepalingen goedgekeurd en de nationale toezichthouders kunnen van geval tot geval hetzelfde doen voor contractbepalingen tussen organisaties of voor bindende bedrijfsvoorschriften voor gegevensverwerking binnen één multinational. In de tweede plaats kan er sprake zijn van een uitzondering waarbij, ondanks het feit dat een passend beschermingsniveau en voldoende privacywaarborgen ontbreken, er toch gegevens doorgegeven kunnen worden aan een verwerker in een derde land, ex art. 26 lid 1 95/46/EG (Article 29 Working Party, 'Working document on a common interpretation of Article 26(1) of Directive 95/46/EG of 24 October 1995', WP 114, p. 7). Dit kan slechts in uitzonderlijke gevallen, namelijk wanneer de gegevens ofwel uit een voor het publiek toegankelijk register komen, er een wettelijke plicht tot doorgifte op de verantwoordelijke rust, of de betrokkene ondubbelzinnig toestemming geeft. De andere gronden voor uitzondering zijn gebaseerd op de noodzakelijkheid van de doorgifte in het licht van contractuele of precontractuele verplichtingen, de uitvoering van een overeenkomst in het belang van de betrokkene, de rechtspleging, een zwaarwegend algemenen belang, of de vrijwaring van een vitaal belang van de betrokkene.
5. Al tijdens de totstandkoming van de Gegevensbeschermingsrichtlijn was het duidelijk dat de VS niet aan het passend beschermingsniveau zou voldoen. De privacybescherming in de Amerikaanse private sector is sectoraal en gebaseerd op een combinatie van wetgeving, regulering en zelfregulering. In de Amerikaanse publieke sector worden privacyrechten van buitenlanders buiten het grondgebied in beginsel niet erkend onder de Amerikaanse constitutie. Daarnaast heeft het Internationaal verdrag inzake burgerrechten en politieke rechten (IVBPR) geen directe werking in de VS en art. 17 IVBPR – dat privacy onderstreept – is niet in nationaal recht omgezet. Het Amerikaanse veiligheidsapparaat heeft verregaande bevoegdheden tot het opslurpen van internetverkeer bij internetknooppunten of uit de databanken van private bedrijven. Klokkenluider Edward Snowden onthulde dat dit laatste op brede schaal gebeurd met gegevens van buitenlanders onder de codenaam PRISM.
6. Toch werd eind jaren negentig de Veiligehavenregeling ontworpen om handel te stimuleren en een papierwinkel voor de gegevensdoorgifte naar Amerika te voorkomen. In ruil voor een toereikendheidsoordeel van de EC ex art. 25 lid 6 95/46/EG, kondigde de Department of Justice uit de VS de Veiligehavenbeginselen af, waar ieder Amerikaans bedrijf dat gegevens uit de EU ontving middels zelfregulering aan moest voldoen (2000/520/EG Beschikking van de Commissie van 26 juli 2000 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende 'Vaak gestelde vragen', die door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd). De Federal Trade Commission hield toezicht op de aangesloten organisaties. De beginselen omvatten normen omtrent kennisgeving, keuze, verdere doorgifte, integriteit van de gegevens, toegang en rechtshandhaving (2000/520/EG Bijlage I). De naleving van de beginselen kan echter worden beperkt voor zover dit nodig is om aan de eisen van de nationale veiligheid, het algemeen belang en rechtshandhaving te

voldoen (2000/520/EG Bijlage I punt 4). Indien de wetgeving van de Verenigde Staten een tegenstrijdige verplichting oplegt, moeten organisaties uit dat land de wet in acht nemen, ongeacht of ze aan de Veiligehavenregeling deelnemen of niet (2000/520/EG Bijlage IV Deel B). In 2015 hadden 4600 organisaties zich bij de regeling aangesloten, waaronder NSA-PRISM-partner Facebook.

7. De Snowden-onthullingen, waar het PRISM-programma uit bleek, waren voor het Europees Parlement reden om op te roepen tot opschorting van het Veiligehavenregeling (LIBE, 'Working Document 4 on surveillance activities with respect to EU data and its possible legal implications on transatlantic agreements and cooperation', 12 December 2013, p. 3). De EC, daarentegen, achtte het voldoende om de onderhandelingen over aanvullende waarborgen met de VS te intensiveren om zo het vertrouwen te herstellen in EU-US gegevensstromen (COM (2013) 846 'Herstel van vertrouwen in de EU-VS gegevensstromen', en de COM (2013) 847 'Werking van de Veiligehavenregeling ('Safe Harbour') uit het oogpunt van EU-burgers en in de EU gevestigde bedrijven'). Te midden van die onderhandelingen ligt er nu de *Schrems*-uitspraak.
8. Bij het vaststellen van de intensiteit van het toezicht door het HvJ EU in de *Schrems* zaak verwijst het HvJ EU naar de *Digital Rights Ireland* zaak (*Digital Rights Ireland Ltd* t. *Ierland,* HvJ EU (GK) 8 april 2014, gev. zaken C-293/12 en C-594/12, «EHRC» 2014/140 m.nt. Koning). In die zaak wordt de intensiteit vastgesteld na een analyse van de betrokken rechten, de inmenging en de zwaarte hiervan, en na beantwoording van de vraag of de wezenlijke inhoud en kern van de rechten en vrijheden geëerbiedigd blijft, en of de inmenging voldoet aan een doel van algemeen belang (*Digital Rights Ireland,* reeds aangehaald, punten 29, 34-44). Pas na dit onderzoek richt het HvJ EU zich op de vraag of de vastgestelde inmenging evenredig is, en bepaalt het of de omvang van de beoordelingsbevoegdheid van de wetgever van de Unie in dit geval beperkt moet worden uitgelegd (*Digital Rights Ireland,* reeds aangehaald, punt 45). Het HvJ EU wijst op de belangrijke rol die gegevensbescherming speelt voor privacybescherming. Het meer overtuigende argument voor het strikte toezicht dat het HvJ EU zich in dit geval toekent, is de verwijzing naar de hierboven omschreven nauwkeurige analyse van de vaststelling en omvang van de inmenging op de fundamentele rechten (*Digital Rights Ireland,* reeds aangehaald, punt 48). Het HvJ EU doet dit onder verwijzing naar de *Marper*-zaak van het Europees Hof voor de Rechten van de Mens (*S. en Marper* t. Het *Verenigd Koninkrijk*, EHRM (GK) 4 December 2008, nr. 30562/04 en 30566/04, «EHRC» 2009/13 m.nt. Koops). Dit laatste Hof beoordeelt de discretionaire bevoegdheid van een lidstaat bij de laatste vaste toetssteen, de noodzakelijkheid in een democratische samenleving. De noodzakelijkheids- en evenredigheidstoets volgt dus na de toetsing van de legitimiteit van het nagestreefde doel en de beoordeling of de maatregel is voorzien bij wet.
9. In de *Schrems*-zaak daarentegen zien we het HvJ EU het toetsingsmoment naar voren trekken, waardoor over het geheel genomen strikter toezicht op het gehele wetgevend proces wordt uitgeoefend en de wetgever minder discretionaire bevoegdheid toe kan komen. Het HvJ EU bepaalt dat het toezicht op een beschikking tot een passend beschermingsniveau strikt dient te zijn vanwege de belangrijke rol van gegevensbeschermingsrecht voor privacybescherming en het grote aantal gedupeerden indien persoonsgegevens worden doorgegeven naar een derde land dat geen waarborgen voor een passend beschermingsniveau biedt (punt 78). Met deze strikte toetsingsbril op bepaalt het HvJ EU welke rechten betrokken zijn, of er sprake is van een inmenging, de noodzakelijkheid en evenredigheid van de inmenging, of de aantasting de wezenlijke inhoud van het grondrecht raakt, en als laatste of de inmenging ontoelaatbaar is gezien alle omstandigheden van het geval (punten 92-98 en 103-104). Het is opvallend dat het HvJ EU na de hele strikte toetsing op een simpele procedure fout wijst, en op basis daarvan de beschikking ongeldig verklaard. De commissie heeft niet vermeld dat de VS daadwerkelijk

op grond van hun nationale wetgeving of hun internationale verbintenissen "waarborgen bieden" voor een passend beschermingsniveau. En daarom kan worden geconcludeerd, aldus het HvJ EU dat de Veiligehavenbeginselen niet aan de vereisten van art. 25 lid 6 95/46/EG voldoen (punten 98, 105-106). In mijn optiek had het HvJ EU prima tot deze conclusie kunnen komen met een marginale toets voor vorm- en procedurele fouten.

10. Desalniettemin is de uitgebreide analyse zeer welkom omdat het HvJ EU belangrijke gegevensbeschermingsconcepten en begrippen nader verklaart. Het HvJ EU bouwt zijn specifieke raamwerk om gegevensbeschermingskwesties te beoordelen verder uit door te onderscheiden tussen de complementaire concepten "doeltreffende en volledige bescherming" en "een hoog niveau van bescherming" (punt 39). Het begrip "doeltreffende en volledige bescherming" stak voor het eerst de kop op in de *Google Spain* zaak uit 2014 (*Google Spain* t. *Costeja,* HvJ EU (GK) 13 mei 2014, zaak C-131/12, «EHRC» 2014/186 m.nt. Van Hoboken). In die zaak speelde het een rol in de beoordeling van de territoriale reikwijdte van de Gegevensbeschermingsrichtlijn en de definitie van de voor de verwerking verantwoordelijke (*Google Spain,* reeds aangehaald, punten 38, 52-53, 58 en 84). In de «EHRC»-annotatie bij deze zaak merkte Van Hoboken de nieuwkomer op en koppelde deze aan het EHRM-beginsel dat grondrechtenbescherming "praktisch en doeltreffend van aard" moet zijn en "niet theoretisch en fictief". Van Hoboken vreesde dat de toevoeging "volledig" het proces van precieze afweging van met elkaar botsende grondrechten zou kunnen verstoren.
11. De AG in de *Ryneš*-zaak onderstreepte het belang van doeltreffendheid van het regelgevend kader en een ruime materiële reikwijdte voor de Gegevensbeschermingsrichtlijn (*Ryneš* t. *Úřad pro ochranu osobních údajů,* HvJ EU 11 december 2014, zaak C-212/13, «EHRC» 2015/47 m.nt. Van der Sloot). Hij gebruikte hierbij het concept van "doeltreffende en volledige bescherming" van grondrechten (Conclusie AG in *Ryneš* t. *Úřad pro ochranu osobních údajů,* 10 juli 2014, zaak C-212/13, punt 26). Het HvJ EU nam deze redenering over maar wisselde de term "doeltreffende en volledige bescherming" in voor een "hoog niveau van bescherming" (*Ryneš,* reeds aangehaald, punten 27-30).
12. Zelf gebruikte het HvJ EU het concept van "doeltreffende en volledige bescherming" voor een tweede keer in de uit 2015 daterende *Weltimmo*-zaak om de ruime territoriale reikwijdte van de Gegevensbeschermingsrichtlijn te onderstrepen (*Weltimmo s.r.o.* t. *Nemzeti Adatvédelmi és Információszabadság Hatóság,* HvJ EU 1 oktober 2015, zaak C-230/14, punten 25 en 30). Het HvJ EU legt daarin uit dat, gelet op de doelstelling van de Gegevensbeschermingsrichtlijn om doeltreffende en volledige bescherming te waarborgen van de fundamentele en om elke vorm van wetsontduiking te voorkomen, de bepalingen die toezien op de territoriale reikwijdte uit de richtlijn niet restrictief mogen worden uitgelegd (*Weltimmo*, reeds aangehaald, punten 25-27 en 29-30).
13. In de *Schrems*-zaak legt het HvJ EU uit dat art. 25 van richtlijn 95/46/EG tot doel heeft het door de Gegevensbeschermingsrichtlijn verleende hoge niveau van bescherming te continueren bij doorgifte van persoonsgegevens naar een derde land (zie ook Conclusie AG, *Maximillian Schrems* t. *Data Protection Commissioner*, 23 september 2015, zaak C-362/14, punt 139). Hiervoor moeten de rechtsnormen extraterritoriaal kunnen gelden, omdat deze anders snel omzeild kunnen worden door gegevens door te geven aan een verwerker in een derde land (punten 72-73 en 96). Zoals ik het nu lees verwijst de "doeltreffende en volledige bescherming van grondrechten" naar de ruime territoriale en extraterritoriale reikwijdte van de Gegevensbeschermingsrichtlijn die erop toeziet dat de normen niet worden omzeild door gegevens uit de EU te sluizen, terwijl het "hoge beschermingsniveau" refereert aan een ruime materiële omvang van de Gegevensbeschermingsrichtlijn en het potentieel gewicht dat art. 7 en 8 Hv in de schaal leggen bij de afweging van verschillende grondrechten en vrijheden.
14. De overweging die waarschijnlijk de meeste langetermijn- en verstrekkende gevolgen zal hebben is punt 94, waarin het HvJ EU uitlegt dat "een regeling op grond waarvan de

autoriteiten veralgemeend toegang kunnen krijgen tot de inhoud van elektronische communicatie [moet] worden beschouwd als een aantasting van de wezenlijke inhoud van het grondrecht op eerbiediging van het privéleven zoals door art. 7 van het Handvest gewaarborgd." Dit houdt in ieder geval in dat derde landen die een vergelijkbaar surveillancebeleid als de VS hebben, niet meer in aanmerking komen voor een positief toereikendheidsoordeel. Daarnaast kan punt 94 invloed hebben op de uitleg en zelfs geldigheid van andere bepalingen in de Gegevensbeschermingsrichtlijn omdat deze uitgelegd moet worden op basis van de grondrechten (*Google Spain*, reeds aangehaald, punt 68 en de daar aangehaalde jurisprudentie).

15. De regeling van art. 26 lid 2 van richtlijn 95/46/EG, die erin voorziet dat gegevens kunnen worden doorgegeven naar verwerkers in derde landen die geen passend beschermingsniveau bieden mits de verantwoordelijke voldoende passende waarborgen instelt, mag in mijn ogen niet worden uitgelegd als een regeling die een aantasting van de wezenlijke inhoud van het grondrecht privacy legitimeert. Structurele gegevensstromen naar derde landen met een vergelijkbaar surveillancebeleid als de VS zullen ook niet meer mogelijk zijn op basis van art. 26 lid 2 van richtlijn 95/46/EG vanwege de strijd met de grondrechten uit het Handvest. Dit standpunt deel ik met de toezichthouder van de Duitse deelstaat Sleeswijk-Holstein. (Positionspapier des ULD zum Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015, C-362/14). De Artikel 29-Werkgroep, waarin de toezichthouders uit de EU zijn verenigd, heeft zich niet uitgelaten over dit punt (Article 29 Working Party, Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14), 16 Okober 2015). De Nederlandse overheid daarentegen, wijst juist op de mogelijkheid van passende contractuele bepalingen en ziet wellicht een oplossing in het uitbreiden van bindende bedrijfsvoorschriften voor gegevensdoorgifte naar bewerkers in de VS (*Kamerstukken II* 2014/15, 32317, 363, p. 10 en 14). De EC wijst enkel op de alternatieve mogelijkheden voor doorgifte ex art. 26 lid 1 en 2 van richtlijn 95/46/EG maar haast zich te zeggen dat het de toezichthouders geen strobreed in de weg wil leggen indien deze de legitimiteit van de doorgifte op basis van deze bepalingen wil onderzoeken (Commissiemededeling inzake de overdracht van persoonsgegevens van de EU aan de VS naar aanleiding van het Schrems arrest COM(2015) 566).
16. Mogelijk schuilt de grootse "adder" onder het gras van overweging 94 in het effect dat de overweging kan sorteren binnen de EU. Op dit moment wordt de surveillanceregelgeving in meerdere EU-lidstaten herzien (Bijvoorbeeld Frankrijk LOI n° 2015-912 du 24 juillet 2015 relative au renseignement (1), Chapitre II Des interceptions de sécurité; en het Verenigd Koninkrijk Draft Communications Data Bill, June 2012). In Nederland betreft dit de herziening van de Wet op de inlichtingen- en veiligheidsdiensten. Het huidig voorstel omvat bepalingen die – net zoals de Amerikaanse regelingen – de autoriteiten veralgemeend toegang geven tot de inhoud van elektronische communicatie om selectiecriteria vast te stellen en te verifiëren om deze op een later moment als zoekcriterium te gebruiken in het surveillancesleepnet (Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX; wettekst (consultatieversie juni 2015) Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..) art. 33-35.)
17. Niettegenstaande dat inlichtingen- en veiligheidszaken van de lidstaten buiten de reikwijdte van het EU recht vallen, kunnen deze nationale veranderingen in het surveillancebeleid de Europese marktintegratie verstoren omdat het zowel de Europese als de nationale wetgever in een lastige positie stelt. Gegevensdoorgifte naar lidstaten met een vergaand surveillancebeleid, leidt ertoe dat de autoriteiten van een andere lidstaat veralgemeend toegang kunnen krijgen tot de inhoud van elektronische communicatie en dit tast de

wezenlijke inhoud aan van het grondrecht op eerbiediging van het privéleven zoals door art. 7 van het Handvest gewaarborgd. Het is lidstaten verboden het vrije verkeer van persoonsgegevens tussen lidstaten te beperken of te verbieden om redenen die verband houden met de bescherming van fundamentele rechten en vrijheden, in het bijzonder privacy, ex art. 1 sub b richtlijn 95/46/EG. Onder deze omstandigheden stelt art. 1 lid 2 van richtlijn 95/46/EG een verbod in dat de uitoefening van de fundamentele rechten en vrijheden beperkt en daarom moet de bepaling in het licht van de grondrechten worden uitgelegd (*Google Spain*, reeds aangehaald, punt 68). Iedere beperking op de grondrechten moet de wezenlijke inhoud van die rechten en vrijheden eerbiedigen ex art. 52 Hv. Nu de veralgemeende toegang juist die wezenlijke inhoud raakt is het de vraag of art. 1 lid 2 van richtlijn 95/46/EG nog wel in lijn is met het Handvest, nu het lidstaten verbiedt haar ingezetenen te beschermen tegen de privacyinbreuken van andere lidstaten.

18. De gegevensdoorgifte vanuit de EU naar de VS lijkt zich in een juridische impasse te begeven. Het gegevensbeschermings- en privacyrecht verschilt te veel aan beide kanten van de plas. Deze conclusie is geheel niet nieuw. Vlak na de inwerkingtreding van de Gegevensbeschermingsrichtlijn riepen velen hetzelfde, toch kwam de EC er uit met behulp van een stevige dosis juridische creativiteit. Zolang de VS hun surveillancesleepnetten niet binnen halen, lijkt een oplossing enkel mogelijk met eenzelfde dosis juridische creativiteit. De de belangen in het vinden van een oplossing zijn groot voor commerciële gegevensverwerkers en voor meeliftende inlichtingendiensten. Allen varen ze wel bij vlotte doorgifte van persoonsgegevens. Het is echter de vraag of een Veiligehavenregeling 2.0 ook vijftien jaar in stand zal blijven, want de wereld kijkt toe en mensenrechtenvoorvechters ontdekken de effectiviteit van een procedure in Luxemburg.

M.E. Koning, ICIS, Radboud Universiteit Nijmegen en Columbia Law School, New York.