

MACHTSSTRIJD OVER PERSOONSGEGEVENS

De zaak *Schrems v. Data Protection Commissioner* van het Europees Hof van Justitie

Bart van der Sloot*

Op 6 oktober 2015 heeft het Hof van Justitie van de Europese Unie uitspraak gedaan in de zaak *Maximillian Schrems tegen Data Protection Commissioner*. De zaak betrof de legitimiteit van de doorvoer van persoonsgegevens van Europese burgers naar landen buiten de EU, in het bijzonder de Verenigde Staten. De Richtlijn bescherming persoonsgegevens stelt dat persoonsgegevens alleen naar derde landen mogen worden doorgevoerd als daar een passend beschermingsniveau wordt gewaarborgd. De Europese Commissie had in een beschikking vastgesteld dat de Verenigde Staten inderdaad een dergelijk beschermingsniveau kent. Het Hof van Justitie heeft deze beschikking echter ongeldig verklaard.

1 Introductie

Weinig rechten zijn zo divers als het recht op privacy en het daaraan verbonden recht op gegevensbescherming. Deze vrijheden zijn in de loop der tijd reeds een aantal keer van kleur verschoten en ook heden ten dage zijn ze nog sterk afhankelijk van niet alleen culturele, maar ook persoonlijke voor- en afkeuren. Wat de ene persoon als privacy-schending ervaart, laat de ander immers koud en vice versa. Deze diversiteit heeft een pluriformiteit aan wet- en regelgeving met betrekking tot privacy- en gegevensbescherming in diverse landen ten gevolg gehad, wat vragen oproept ten aanzien van de handhaving van die regels.¹ Niet alleen zijn internetbedrijven vaak niet aan landsgrenzen gebonden, ook ontwikkelingen als *the Internet of Things* en *Cloud Computing* dragen er in hoge mate aan bij dat gegevens vaak razendsnel tussen verschillende jurisdicties worden verplaatst en uitgewisseld. De meest prangende vraag die zich momenteel aandient, is hoe de Europese rechten van burgers kunnen worden gehandhaafd als Amerikaanse bedrijven en overheidsorganisaties toegang hebben tot persoonsgegevens, terwijl zij zich niet of nauwelijks gebonden achten aan de Europese regels. De Verenigde Staten kennen wel regels aangaande privacy- en gegevensbescherming, maar die worden doorgaans als veel minder stringent en bindend ervaren dan hun Europese tegenhangers.

Om dit euvel te voorkomen is in de Richtlijn bescherming persoonsgegevens (hierna ook: de Richtlijn)² bepaald dat Europese persoonsgegevens niet naar derde landen mogen worden doorgevoerd

als er in dat land geen passend beschermingsniveau geldt. Wel stelt de Richtlijn dat de Europese Commissie (hierna: de Commissie) een oordeel kan vellen over dit passende beschermingsniveau:

'De Commissie kan volgens de procedure van artikel 31, lid 2, constateren dat een derde land, op grond van zijn nationale wetgeving of zijn internationale verbintenissen, die het met name na de in lid 5 bedoelde onderhandelingen is aangegaan, waarborgen voor een passend beschermingsniveau in de zin van lid 2 biedt met het oog op de bescherming van de persoonlijke levenssfeer en de fundamentele vrijheden en rechten van personen. De Lidstaten nemen de nodige maatregelen om zich naar het besluit van de Commissie te voegen.'³

De Commissie heeft inderdaad een beschikking uitgevaardigd waarin nadere bepalingen staan en waarin wordt gesteld dat de Verenigde Staten inderdaad een passend beschermingsniveau kent.⁴ Dit wordt ook wel de *safe harbor agreement* genoemd. Een Europese burger (Max Schrems) betwijfelt echter of de Verenigde Staten inderdaad een passend beschermingsniveau kent. Hij dient een klacht in bij de Ierse Data Protection Authority (vergelijkbaar met het Nederlandse College Bescherming Persoonsgegevens) en vervolgens, na in het ongelijk te zijn gesteld, bij de nationale rechter. Deze rechter besluit een prejudiciële vraag aan het Europees Hof van Justitie (hierna ook: HvJ) te stellen. De uitspraak van het HvJ is kort gezegd dat de beschikking van de Commissie ongeldig is.⁵ Dit kan verregaande consequenties hebben voor de mogelijkheid van Amerikaanse bedrijven en instanties om gegevens over Europese burgers te verwerken.

* Mr.dr.s. B. van der Sloot is onderzoeker aan het Instituut voor Informatierecht, Universiteit van Amsterdam. Dit artikel is afgerond op 13 februari 2016.

- 1 Zie o.a.: L.A. Bygrave, *Data Privacy Law: An International Perspective*, Oxford: Oxford University Press 2014.
- 2 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (*PbEU* 1995, L 281), p. 31-50.
- 3 Art. 25 lid 6 Richtlijn bescherming persoonsgegevens.
- 4 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 Veiligheidsbeginselen 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 (Kennisgeving geschied onder nummer C(2000) 2441). Zie ook: Europese Commissie, Mededeling van de Commissie aan het Europees Parlement en de Raad: Herstel van vertrouwen in de gegevensstromen tussen de EU en de VS, COM(2013) 846 final, Brussel, 27.11.2013.
- 5 HvJ EU 6 oktober 2015, ECLI:EU:C:2015:650, C-362/14 (*Maximillian Schrems tegen Data Protection Commissioner*, in tegenwoordigheid van: *Digital Rights Ireland Ltd*).



Foto: Nancy Wolter © Ars Aequi

Persoonsgegevens zijn steeds belangrijker geworden, niet alleen in verband met criminaliteits- en terrorismebestrijding, ook zijn deze gegevens de belangrijkste bezittingen van bedrijven als Google, Apple, Facebook en Twitter

2 Machtsstrijd over persoonsgegevens

Naast de juridische, is het belangrijk om ook de politieke dimensie van dit vraagstuk in ogenschouw te nemen. In feite zijn persoonsgegevens steeds belangrijker geworden, niet alleen in verband met criminaliteits- en terrorismebestrijding, ook zijn deze gegevens de belangrijkste bezittingen van bedrijven als Google, Apple, Facebook en Twitter. Er is dan ook al langer een strijd gaande omtrent het bezit van en de zeggenschap over deze gegevens. Uiteraard vechten de Verenigde Staten en Europa om deze macht. De strijd leek lange tijd in het voordeel van de Verenigde Staten te worden beslecht, omdat zowel overheidsinstanties als de NSA en bedrijven als Google en Facebook op grote schaal gegevens verzamelen van Europese burgers en daarbij de Europese regels grotendeels negerden. Europa is de laatste tijd echter met een opmars bezig. Niet alleen de zaak *Schrems* is daar een voorbeeld van, ook de *Google Spain*-zaak van het Hof van Justitie is van belang.⁶ Daarin werd niet alleen het recht om vergeten te worden aangenomen, ook werd bepaald dat Google gewoon onderworpen is aan de Europese regelgeving, ook al

is zijn hoofdkantoor in de Verenigde Staten gevestigd. Tevens wordt de huidige Richtlijn bescherming persoonsgegevens op korte termijn vervangen door de Algemene Verordening Gegevensbescherming (hierna: Verordening),⁷ die strengere regels kent en verregaande bevoegdheden aan handhavende organisaties toekent om de Europese regels af te dwingen en schendingen te bestraffen.

Daarnaast is er een strijd tussen de publieke en de private sector omtrent wie de macht en zeggenschap kan claimen over de persoonsgegevens. Enerzijds moet worden opgemerkt dat technologiebedrijven als Google en Facebook, maar ook intelligence-bedrijven als Palantir, vaak vooroplopen in de ontwikkeling van nieuwe technologieën en toepassingen. Ook is er een privatisering gaande ten aanzien van de verzameling en verwerking van persoonsgegevens, zelfs als het gaat om de opsporing van criminelen en terroristen. Vaak worden bedrijven ingehuurd om informatiesystemen op te zetten, data-analyses uit te voeren of worden medewerkers van dergelijke private ondernemingen langdurig gedetacheerd bij overheidsdiensten om de gegevensverwerking ter hand te nemen, zoals bijvoorbeeld het geval was met Edward Snowden. In Nederland is onder andere bekend dat de AIVD nauw samenwerkt met een bedrijf als Fox-IT.⁸ Deze verregaande vorm van privatisering wordt ook weleens 'surveillance-capitalism' genoemd.⁹ Aan de andere kant zijn overheidsdiensten vaak in staat om zich met behulp van al dan niet legale middelen toegang te verschaffen tot de gegevens die door bedrijven worden verzameld, zoals door het plaatsen van taps op internet- en telefoonkabels. Tevens hebben zij, met een beroep op terrorismebestrijding en de nationale veiligheid, vaak een wettelijke grondslag om zeer grote hoeveelheden persoonsgegevens van bedrijven te vorderen.¹⁰ Ook als zij een dergelijke

6 HvJ EU 13 mei 2014, ECLI: EU:C:2014:317, C-131/12 (*Google Spain SL, Google Inc. tegen Agencia Española de Protección de Datos (AEPD), Mario Costeja González*).

7 www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf.

8 www.fox-it.com/nl.

9 S. Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization', *Journal of Information Technology* 2015, afl. 30, p. 75-89.

10 Zie o.a. de US Patriot Act, HR 3162 RDS, 107th Congress, 1st Session, H. R. 3162, In the Senate of the United States, October 24, 2001.

grondslag missen kunnen zij bedrijven verzoeken om gegevens af te staan – de praktijk leert dat de meeste bedrijven medewerking verlenen als de FBI, CIA of NSA op de stoep staat.

De praktijk leert dat de meeste bedrijven medewerking verlenen als de FBI, CIA of NSA op de stoep staat

Ook is er binnen Europa een strijd gaande over competentie tussen Europese instituties en nationale organen. Traditioneel had Europa weinig zeggingskracht over de verwerking van persoonsgegevens voor veiligheidsdoelinden, onder meer vanwege de drie-pijler-structuur. Zo is op dergelijke gegevensverwerking niet de Richtlijn bescherming persoonsgegevens van toepassing, maar een besluit van de Europese Raad,¹¹ dat zowel minder stringent als minder dwingend is naar lidstaten. Voor nationale veiligheid en terrorismebestrijding geldt te meer het prerogatief van nationale lidstaten. Ook de Richtlijn bescherming persoonsgegevens geeft de lidstaten de nodige ruimte, omdat het aan landen zelf is om de regels in hun nationale wetgeving te implementeren – er bestaat dan ook een grote diversiteit in de EU op dit punt. Aan de andere kant wordt de macht van nationale instanties steeds verder ingeperkt. Zo wordt de Richtlijn vervangen door een verordening, die directe werking heeft, wordt de beslissing van de Europese Raad op termijn vervangen door een richtlijn op hetzelfde punt,¹² is de drie-pijler-structuur verlaten en wordt er ook in het kader van nationale veiligheid en terrorismebestrijding (noodgedwongen) steeds meer samengewerkt tussen nationale overheden op Europees niveau. Ook het Hof van Justitie trekt steeds meer bevoegdheid naar zich toe en wordt activistisch op diverse terreinen, zodat de macht van nationale instanties verder wordt ingeperkt.

Er zijn binnen Europa tal van instituties en organen die zich op dit terrein willen positioneren en profileren

Vervolgens moet ook worden bedacht dat er binnen Europa tal van instituties en organen zijn die zich op dit terrein willen positioneren en profileren. Zo is er ten aanzien van de totstandkoming van de Verordening een interessant steekspel te zien geweest. De Commissie kwam met het voorstel voor deze Verordening, deels om sier te maken met privacy-rechten als het recht om vergeten te worden, het recht op dataportabiliteit en het recht om *profiling* te blokkeren.¹³ Het Europese Parlement overtrof de Commissie vervolgens en kwam met een zeer verregaand voorstel dat nog meer en betere bescherming bood aan de rechten en vrijheden van burgers.¹⁴ De Europese Raad, waarin de ministers van de diverse lidstaten zitting hebben, ging dit echter weer te ver en kwam met een afgezwakt voorstel.¹⁵ Vervolgens is er lange tijd onderhandeld tussen deze drie partijen

en is er een compromis tot stand gekomen. Opmerkelijk was ook de positie van de European Data Protection Supervisor (EDPS), de waakhond van gegevensbescherming binnen de EU-instanties zelf, die eigenlijk dus slechts een zeer beperkte rechtsbevoegdheid heeft. De EDPS kwam met een eigenstandig voorstel, dat het naast de drie al liggende voorstellen plaatste.¹⁶ Daarmee overtoepte zij op haar beurt de zogenoemde Artikel 29 Werkgroep, ook wel Werkgroep 29. Dat is de officiële organisatie die is ingesteld middels artikel 29 van de Richtlijn bescherming persoonsgegevens. In deze werkgroep zitten vertegenwoordigers van alle nationale handhavende organisaties (de Data Protection Authorities, DPA's); alhoewel zij weinig juridische middelen heeft, geeft zij wel adviezen over tal van onderwerpen (zoals over de Verordeningvoorstellen), die doorgaans als zeer zwaarwegend worden aangemerkt. Alhoewel de EDPS deze slag wellicht heeft gewonnen moet tevens worden opgemerkt dat de Werkgroep 29 met de inwerkingtreding van de Verordening zal transformeren tot de European Data Protection Board, die veel meer (juridische) macht en middelen zal krijgen.

Alhoewel het Europees Hof voor de Rechten van de Mens lange tijd gold als de hoeder van privacy en gegevensbescherming in Europa, probeert het Hof van Justitie zich de laatste tijd steeds meer te positioneren op dit terrein

Tot slot moet ook worden bedacht dat er een strijd gaande is tussen de Raad van Europa en de Europese Unie. Traditioneel was er een onderscheid tussen de twee organisaties. Waar de Raad van Europa zich voornamelijk bezighield met fundamentele vrijheden en mensenrechten, was de EU primair gericht op economische terreinen. Zo had de EU-Richtlijn bescherming persoonsgegevens een economische grondslag, namelijk het reguleren van de vrije doorvoer van persoonsgegevens en kent zij officieel twee doeleinden: de bescherming van persoonsgegevens en het vrije verkeer van persoonsgegevens. Traditioneel nam de Raad van Europa dus het voortouw op het gebied van privacy en gegevensbescherming, maar langzamerhand probeert de EU zich steeds meer op dit terrein te profileren. Terwijl het Europees Verdrag tot de Rechten van de Mens van de Raad van Europa uit 1950 in artikel 8 reeds het recht op privacy erkende,¹⁷ heeft de Europese Unie in 2000 het Handvest van de grondrechten van de Europese Unie aangenomen, waarin in artikel 7 en 8 het recht op privacy en gegevensbescherming wordt geregeld.¹⁸ Terwijl de Raad van Europa al in de jaren zeventig de eerste gegevensbeschermingsregels neerlegde¹⁹ en in 1981 met de Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data een internationale standaard neerzette,²⁰ heeft de EU in 1995 de daar zeer nauw op aansluitende Richtlijn bescherming persoonsgegevens aangenomen.²¹ Alhoewel het Europees Hof voor de Rechten van de Mens lange tijd

11 Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politieke en justitiële samenwerking in strafzaken. Deze zal op termijn worden vervangen door een richtlijn.

12 Zie o.a.: Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data /* COM/2012/010 final – 2012/0010 (COD).

13 http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

14 Zie o.a.: www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2013-0402&language=EN.

15 Zie o.a.: <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/nl/pdf>.

16 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/hared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_Annex_EN.pdf.

17 Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden, Rome, 4.XI.1950.

18 Handvest van de Grondrechten van de Europese Unie, 2000/C 364/01, 18.12.2000.

19 <https://wcd.coe.int/com.intranet.InstraServlet?command=com.intranet.CmdBlobGet&IntranetImage=589402&SecMode=1&DocId=646994&Usage=2>. <https://wcd.coe.int/com.intranet.InstraServlet?command=com.intranet.CmdBlobGet&IntranetImage=590512&SecMode=1&DocId=649498&Usage=2>.

20 www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

21 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (*PbEU* 1995, L 281), p. 31-50.

gold als de hoeder van privacy en gegevensbescherming in Europa, probeert het Hof van Justitie zich de laatste tijd steeds meer te positioneren op dit terrein, waarbij onder meer kan worden gewezen op de 'right to be forgotten'-zaak,²² de dataretentiezaak²³ en de onderhavige *Schrems*-zaak.

Het HvJ oordeelt dat de beschikking van de Commissie krachtens artikel 288, vierde alinea van het Verdrag betreffende de Werking van de Europese Unie verbindend is voor alle lidstaten tot wie zij is gericht

3 De zaak *Schrems*

Terug naar de zaak *Schrems* en de juridische vraagstukken die daarin centraal stonden. Het verloop van de zaak is relatief simpel. Een Oostenrijkse ingezetene genaamd Max Schrems is sinds 2008 gebruiker van Facebook. Degenen die op het grondgebied van de Unie wonen en Facebook willen gebruiken, moeten bij hun inschrijving een overeenkomst ondertekenen met Facebook Ireland, een dochteronderneming van Facebook Inc., die zelf in de Verenigde Staten is gevestigd. De persoonsgegevens van de gebruikers van Facebook die op het grondgebied van de Unie wonen, worden geheel of gedeeltelijk doorgegeven naar servers van Facebook Inc. die zich op het grondgebied van de Verenigde Staten bevinden. Op 25 juni 2013 heeft Schrems bij de Ierse Commissioner een klacht ingediend, waarin hij de Commissioner vroeg om Facebook Ireland te verbieden om zijn persoonsgegevens naar de Verenigde Staten door te geven, gezien onder meer de onthullingen van Snowden over de NSA. Van oordeel dat zij niet verplicht was tot onderzoek van de feiten, heeft de Commissioner die klacht afgewezen omdat zij grondslag miste. De Commissioner was van oordeel dat er geen bewijs was dat de NSA zich toegang tot de persoonsgegevens van de betrokkene had verschafte. Bovendien stelde hij dat elke vraag betreffende de gepastheid van de bescherming van persoonsgegevens in de Verenigde Staten in overeenstemming met beschikking 2000/520 moest worden beantwoord en dat de Commissie in die beschikking had geconstateerd dat de Verenigde Staten waarborgen voor een passend beschermingsniveau boden. De High Court, waar beroep werd aangetekend door Schrems, was evenwel kritischer en stelde het HvJ daarom prejudiciële vragen. Daarbij gaat het met name om de vraag of een DPA klachten in ontvangst kan nemen van burgers betreffende de geldigheid van de beschikking van de Commissie of over zaken die daaruit voortvloeien en of de rechter, ofwel nationaal ofwel het Hof van Justitie, hier een oordeel over kan vellen.

Het HvJ oordeelt dat de beschikking van de Commissie krachtens artikel 288, vierde alinea van het Verdrag betreffende de Werking van de Europese Unie²⁴ verbindend is voor alle lidstaten tot wie zij is gericht, zodat zij ook verbindend is voor hun organen, in die zin dat zij tot gevolg heeft dat de doorgifte van persoonsgegevens vanuit de lidstaten naar het daarin

genoemde derde land wordt toegestaan. Zolang de beschikking van de Commissie niet door het HvJ ongeldig is verklaard, mogen de lidstaten en hun organen, waaronder de onafhankelijke toezichhoudende autoriteiten, dan ook geen maatregelen treffen die met deze beschikking in strijd zijn, zoals handelingen die tot doel hebben om dwingend vast te stellen dat het derde land waarop de beschikking ziet, geen waarborgen voor een passend beschermingsniveau biedt. De handelingen van de instellingen van de Unie worden immers in beginsel vermoed rechtmatig te zijn en dus rechtsgevolgen in het leven te roepen, zolang zij niet zijn ingetrokken, in het kader van een beroep tot nietigverklaring nietig zijn verklaard of ten gevolge van een prejudiciële verwijzing of een exceptie van onwettigheid ongeldig zijn verklaard. Het HvJ benadrukt zijn eigen positie door te stellen dat uit vaste rechtspraak volgt dat de Unie een door het recht beheerste unie is waarin de handelingen van de instellingen met name aan de Verdragen, de algemene rechtsbeginselen en de grondrechten worden getoetst. De beschikkingen van de Commissie kunnen dus niet aan die toetsing ontsnappen. Dit in aanmerking nemend, is het HvJ als enige bevoegd om de (on)geldigheid van de beschikking van de Commissie vast te stellen. Wel heeft de burger de mogelijkheid om een klacht in te dienen bij nationale instanties. Zowel de DPA's als de nationale rechters mogen de rechtsgeldigheid van besluiten onderzoeken, maar hen komt niet de competentie toe hier een uiteindelijk oordeel te vellen. Een DPA kan de zaak voorleggen aan een nationale rechter en deze kan die op haar beurt weer voorleggen aan het Hof van Justitie.

Het HvJ is kritisch op tal van punten uit de beschikking van de Commissie. Het is onduidelijk of het op één van deze punten de beschikking ongeldig verklaart of dat het de combinatie van factoren is

Dit is het meer principiële gedeelte van de uitspraak van het HvJ; het vervolgt met een concrete analyse ten aanzien van de geldigheid van de voorliggende beschikking van de Commissie. Dit oordeel valt negatief uit – het HvJ verklaart de beschikking ongeldig wegens strijd met het Unierecht. Het leest daarbij de Richtlijn bescherming persoonsgegevens in samenhang met het recht op privacy en het recht op gegevensbescherming, artikel 7 en 8 van het Handvest van de Europese Unie en artikel 47 van datzelfde Handvest dat stelt:

'Eenieder wiens door het recht van de Unie gewaarborgde rechten en vrijheden zijn geschonden, heeft recht op een doeltreffende voorziening in rechte, met inachtneming van de in dit artikel gestelde voorwaarden. Eenieder heeft recht op een eerlijke en openbare behandeling van zijn zaak, binnen een redelijke termijn, door een onafhankelijk en onpartijdig gerecht dat vooraf bij wet is ingesteld. Eenieder heeft de mogelijkheid zich te laten adviseren, verdedigen en vertegenwoordigen. Rechtsbijstand wordt verleend aan diegenen die niet over toereikende financiële middelen beschikken, voorover die bijstand noodzakelijk is om de daadwerkelijke toegang tot de rechter te waarborgen.'

²² HvJ EU 13 mei 2014, ECLI: EU:C:2014:317, C-131/12.

²³ HvJ EU 8 april 2014, C-594/12 (*Digital Rights Ireland Ltd (C-293/12) tegen Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, in tegenwoordigheid van: Irish Human Rights Commission, en Kärntner Landesregierung (C-594/12)*, Michael Seitzinger, Christof Tsochoglou e.a.).

²⁴ <http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex%3A12012E%2FTXT>.

Het HvJ is kritisch op tal van punten uit de beschikking van de Commissie. Het is onduidelijk of het op één van deze punten de beschikking ongeldig verklaart (en zo ja op welk punt) of dat het de combinatie van factoren is (en zo ja wat de weging is tussen de verschillende factoren). Het bespreekt met name artikel 1 en 3 van de beschikking en komt op basis daarvan tot zijn negatieve oordeel. Het vervolgt door te stellen dat aangezien 'de artikelen 1 en 3 van beschikking 2000/520 onlosmakelijk verbonden zijn met de artikelen 2 en 4 en met de bijlagen daarbij, [...] hun ongeldigheid tot gevolg [heeft] dat de geldigheid van deze beschikking in haar geheel is aangetast.'²⁵

De belangrijkste punten die het HvJ noemt ten aanzien van artikelen 1 en 3 zijn dat er wordt gewerkt met een mechanisme van zelfcertificering, terwijl er niet of nauwelijks wordt gecontroleerd hoe het gesteld is met de betrouwbaarheid van deze certificaten. Daarnaast geldt er in de Verenigde Staten een zeer brede bevoegdheid voor overheidsdiensten om in het kader van de van nationale veiligheid gegevens te verzamelen en te verwerken, terwijl deze bevoegdheid met weinig waarborgen is omkleed. Ook de klachtenprocedure en mogelijkheid voor burgers om in bezwaar en beroep te komen zijn te beperkt en derhalve in strijd met artikel 47 van het Handvest. Tot slot worden ook de bevoegdheden van de DPA's om onderzoek te doen naar en naar aanleiding van klachten van datasubjecten beperkt, wat in strijd is met de Richtlijn bescherming persoonsgegevens. Alhoewel de Commissie de macht heeft om een oordeel te vellen over het passende beschermingsniveau van een land (en daarmee over de materiële bepalingen uit de Richtlijn), kan het niet derogeren aan de bevoegdheden van de DPA's zoals ten aanzien van onderzoek, naleving en handhaving.

De mogelijke gevolgen van deze uitspraak van het Hof van Justitie zijn groot, nu het voorlopig onduidelijk is of gegevensdoorvoer naar Amerika wel legitiem is

4 Conclusie

De mogelijke gevolgen van deze uitspraak van het Hof van Justitie zijn groot, nu het voorlopig onduidelijk is of gegevensdoorvoer naar Amerika wel legitiem is. Daarmee komt niet alleen de positie van Amerikaanse bedrijven, maar ook die van Europese bedrijven die in Amerika zijn gevestigd en die van Europese overheidsorganisaties die samenwerken met ofwel Amerikaanse bedrijven ofwel Amerikaanse overheidsinstanties onder druk te staan. Bij de afronding van dit artikel werd net bekend dat de EU en de VS een akkoord hebben bereikt over een nieuwe, aangepaste 'safe harbor agreement'.²⁶ Welke aanpassingen hierin zijn vervat, is nochtans onduidelijk en ook is ongewis of deze nieuwe regels de toets der kritiek van het Hof van Justitie zullen doorstaan. D66-Europarlementariër Sophie in 't Veld stelde in ieder geval:

'Dit gaat niet standhouden in de rechtbank. De deal is gemaakt onder immense druk van de VS, hun geheime dienst en het Amerikaanse bedrijfsleven. Het Europees Hof is heel duidelijk in waar de grenzen liggen, en de garanties die nu op papier worden gegeven hebben juridisch gezien geen enkele waarde.'²⁷

Het onderwerp van transnationale dataverwerking en gegevensdoorvoer zal derhalve voorlopig nog wel even op de politieke agenda blijven staan.

²⁵ HvJ EU 6 oktober 2015, ECLI:EU:C:2015:650, C-362/14 (*Maximilian Schrems tegen Data Protection Commissioner, in tegenwoordigheid van: Digital Rights Ireland Ltd*), r.o. 105.

²⁶ http://europa.eu/rapid/press-release_IP-16-216_en.htm.

²⁷ www.rtlnieuws.nl/economie/home/eu-en-vs-sluiten-politieke-deal-om-je-data-te-beschermen.