Het papieren schild

Over de beschermingswaarde van het EU-VS-privacyschild tegen niet-noodzakelijke of disproportionele datacollectie door de VS-inlichtingen- en politiediensten

Gert Vermeulen[a]

Panopticon, 37 (3), 185-196
 | ISSN 0771-1409 | Mei 2016

[a] Hoogleraar strafrecht en directeur *Institute for International Research on Criminal Policy* (IRCP) (www.ircp.org), Vakgroep Criminologie, Strafrecht en Sociaal Recht, Universiteit Gent; bijzonder hoogleraar 'Evidence', Universiteit Maastricht; commissaris, Commissie voor de Bescherming van de Persoonlijke Levenssfeer (Corresp.: Gert.Vermeulen@UGent.be).

Inleiding

Na de aanslagen van de jongste week op de nationale luchthaven en in het metrostation Maalbeek – en de vragen die naar aanleiding ervan zijn gerezen in verband met een mogelijk gebrekkige informatiepositie, -exploitatie of -deling op het niveau van de inlichtingen- of politiediensten – kan een kritisch stuk over de balans tussen datacollectie en privacy een vreemde keuze lijken. Niemand betwijfelt evenwel dat privacy moet wijken wanneer dat noodzakelijk is en proportioneel om (Jihadistisch) terrorisme te voorkomen of te bestrijden. Daar gaat dit stuk ook niet over. Wel over de schokkend zware prijs die de EU op het punt staat welwillend te betalen op het vlak van de fundamentele waarden die de grondrechten van de EU-burger inzake privacy en dataprotectie uitmaken. In tijden van terrorisme is zin voor nuance moeilijk, maar des te meer nodig.

1. Inadequatie van het VS-dataprotectieregime: na Snowden voor iedereen helder

In de nasleep van 9/11 sloten de EU en de VS een aantal overeenkomsten, o.m. inzake de uitwisseling van persoonsgegevens tussen Europol en de VS en inzake de justitiële uitwisseling van persoonsgegevens in het kader van de wederzijdse rechtshulp in strafzaken. Twaalf jaar geleden reeds werd in dit tijdschrift geopperd dat de EU zich met deze – toen nieuwe – trans-Atlantische rechtsinstrumenten had laten ringeloren en zijn eigenheid op het stuk van privacy had prijsgegeven (Vermeulen, 2004). De analyse toen was dat de EU te ver was meegegaan in een logica die terrorisme primair vanuit een oorlogsratio beziet. Inzonderheid werd vastgesteld dat noch politieel, noch justitieel de adequatie van het VS-dataprotectieniveau was aangetoond, hoewel zowel de toenmalige Europol-Overeenkomst als Dataprotectierichtlijn 95/46 dat vereisten. Doelbinding (of specialiteit) bij de aanwending van verstrekte gegevens bleek in de trans-Atlantische politie- en justitiehuishouding immers een zo goed als inhoudsloos concept geworden, waarbij de VS informatie die in strafzaken

was verstrekt vrij konden inwisselen voor louter administratieve of inlichtingendoeleinden. Ook nadat de EU in december 2008 via Kaderbesluit een geëigend dataprotectiekader voor politie en justitie had uitgewerkt, moest opnieuw worden vastgesteld dat het de EU niet menens was met de adequatievereiste voor het gegevensbeschermingsregime van derde landen (De Busser & Vermeulen, 2010). De toenmalige Toekomstgroep Binnenlandse Zaken, die op dat eigenste moment begonnen was het Programma van Stockholm (het derde EU-vijfjarenplan justitie en binnenlandse zaken) voor te bereiden, ging gemakshalve zelfs uit van de principiële adequatie van het VS-dataprotectieregime en lanceerde ineens de idee van een trans-Atlantische ruimte van vrijheid, veiligheid en rechtvaardigheid. Zover kwam het toen (nog) niet.

Intussen was overigens al enige jaren duidelijk dat de VS massaal (Europese) persoonsgegevens capteerden. In 2006 was immers onthuld dat het ministerie van financiën van de VS zich via administratieve dwangbevelen ten aanzien van de VS-hub van de in Tervuren gevestigde *Society for Worldwide Interbank Financial Telecommunication* (SWIFT) toegang verschaften tot het wereldwijde giraal betaalverkeer, in het kader van de strijd tegen de financiering van terrorisme en ongetwijfeld ook voor andere (inclusief economische) doelen. Ook SWIFT zelf was daarbij trouwens in de fout gegaan, want de hub die het in de VS o.m. als back-up-faciliteit had ingesteld, had de zogenaamde *Safe Harbour*-principes niet onderschreven. Die principes waren in 2000 door de Europese Commissie uitgewerkt opdat, nu het VS-gegevensbeschermingsregime op zich niet als passend of adequaat kon worden bestempeld, er niettemin commercieel gegevensverkeer tussen de EU en de VS zou mogelijk zijn. Bedrijven die aangaven (en zich als zodanig zelfcertificeerden) de in de *Safe Harbour*-beschikking van de Commissie neergelegde principes na te leven, golden als een vanuit privacy-oogpunt 'veilige haven' in de VS, waarnaar Europese bedrijven dus gegevens mochten overmaken. Dat was evenwel niet het geval voor de SWIFT-hub in de VS, zodat het Belgische bedrijf er geen back-up-data had mogen localiseren. De reactie van de EU op het schandaal was allesbehalve overtuigend. Intra-Europese betalingsverrichtingen werden weliswaar niet langer naar de VS-hub gestuurd (ook al had SWIFT die intussen wel als 'veilige haven' geregistreerd), maar de Commissie onderhandelde namens de EU een akkoord met de VS waarbij die via een Europol-filter (die weinig om het lijft heeft) alsnog geval per geval *bulk*toegang tot het intra-Europese betalingsverkeer kunnen krijgen. Die – in 2010 afgesloten – TFTP-overeenkomst (*Terrorist Financing Tracking Program*) bevat overigens een artikel waarin het ministerie van financiën axiomatisch adequaat wordt verklaard wat gegevensbeschermingsniveau betreft. Gegeven de brede data-*sharing* tussen allerlei VS-overheidsdiensten (in strijd met het Europese finaliteitsprincipe) kon over de *in*adequatie van het VS-dataprotectieregime op dat moment nochtans al lang geen twijfel meer bestaan. Dat de *Foreign Intelligence Surveillance Act* (FISA), zoals na 9/11 gewijzigd door de *Patriot Act* en in 2008 nog verder uitgebreid, de VS toelieten om zowel zonder als met rechterlijk bevel disproportioneel, wereldwijd en in bulk elektronische communicatie te monitoren, was ook helder (zie o.m. De Busser, 2009). Een en ander werd in de zomer 2013 bevestigd door de onthullingen van klokkenluider Edward Snowden. Die choqueerden vooral door de *ampleur* van de afluisterpraktijken van de NSA (*National Security Agency*) – o.m. via het PRISM-programma – en de Britse inlichtingendienst GCHQ (*Government Communications Headquarters*) – die jarenlang *Belgacom International Carrier Service* (Bics) bespioneerde. Als dochteronderneming van het huidige *Proximus* levert Bics wereldwijd hardware waarlangs elektronische communicatie (internet-, telefonie-, gsm- en smsverkeer) van telecombedrijven en overheidsinstellingen loopt. De intense onderlinge samenwerking tussen NSA en GCHQ en binnen de zogenaamde Five Eyes Community (met de inlichtingendiensten van Canada, Australië en Nieuw-Zeeland) werd er ook door bevestigd, ook al wisten we natuur-

lijk dat de vijf in het kader van Echelon al decennialang het wereldwijde satellietcommunicatieverkeer afluisterden, inclusief voor commerciële doeleinden. Het Europees Parlement had er zelfs in 2000 reeds een heuse onderzoekscommissie naar ingesteld, en interne NSA-nieuwsbrieven die in het kader van verdere Snowden-onthullingen in de zomer van 2015 bekend raakten, hebben de bevestiging ervan van de kant van de VS geleverd.

2. *Safe Harbour* toch geen veilige haven

Het was de vorige justitiecommissaris Reding menens met een verbeterde privacybescherming in de EU. Gebruik makend van de kapstok die het Verdrag van Lissabon haar had aangereikt, lanceerde ze begin 2012 een ambitieus privacywetgevingspakket. Een nieuwe Verordening moest de oude Richtlijn 95/46 vervangen en o.m. de (VS-)aanbieders van diensten op EU-grondgebied aan Europese dataprotectieregels binden. Een nieuwe Richtlijn moest het Kaderbesluit van 2008 inzake dataprotectie in de sfeer van politie en justitie upgraden. Na veel vijven en zessen – en bijna vier jaar en een Europese Commissie later – was het dan zover: in december 2015 werd politiek akkoord bereikt over de nieuwe Verordening en Richtlijn. Tegen de zomer worden ze formeel aangenomen, en twee jaar later moeten de lidstaten ze al gaan toepassen. Zonder meer een opsteker. De adequatie-eis voor gegevenstransfers naar derde landen blijft overigens intact.

Reding ging ook in de verdediging van de EU-burger wat de toegang door de VS tot diens gegevens betreft. Eind november 2013 – luttele maanden na de Snowden-onthullingen – kwam ze met twee parallelle mededelingen: 'Herstel van vertrouwen in de gegevensstromen tussen de EU en de VS' (COM(2013) 846 final) en 'Mededeling betreffende de werking van de veiligehavenregeling ('Safe Harbour') uit het oogpunt van EU-burgers en in de EU gevestigde ondernemingen' (hierna: *Safe Harbour*-mededeling) (COM(2013) 847 final). De eerste mededeling ging vergezeld van een verslag met de 'bevindingen over de ad-hocwerkgroep Gegevensbescherming van de EU en de VS', en stipte o.m. aan dat de verbeteringen in de *Safe Harbour*-beschikking betrekking zouden moeten hebben op 'de structurele tekortkomingen in verband met de transparantie en de handhaving, de materiële veiligehavenbeginselen en de werking van de *uitzondering inzake de nationale veiligheid*'. De *Safe Harbour*-beschikking bepaalde immers expliciet dat de 'eisen van *nationale veiligheid, algemeen belang en rechtshandhaving'* van de VS voorrang hebben op de *Safe Harbour*-principes Principes (bijlage I, vierde alinea). Die uitzonderingen bleken de veilige havens dus onveilig te maken. In haar *Safe Harbour*-mededeling stelde de Commissie vast dat '[a]lle 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, [...] bijvoorbeeld gecertificeerd [lijken] te zijn in het kader van de veilige haven', waardoor die dus 'een van de kanalen [is geworden] waarlangs de Amerikaanse inlichtingendiensten toegang hadden tot persoonsgegevens die oorspronkelijk in de EU waren verwerkt' (punt 7). Dat was ook zo: *Microsoft, Google, Facebook, Apple, Yahoo!, Skype, YouTube* ... allemaal waren ze zelfgecertificeerd onder *Safe Harbour* én betrokken in het PRISM-programma. De Commissie besloot dat '[h]et grootschalige karakter van deze programma's [...] tot gevolg [kon] hebben dat *meer* gegevens die in het kader van de veilige haven zijn doorgegeven, door de Amerikaanse autoriteiten [werden] geraadpleegd en verder verwerkt *dan strikt noodzakelijk is voor en evenredig is met de bescherming van de nationale veiligheid*, zoals de uitzondering waarin de veiligehavenbeschikking voorziet, bepaalt' [eigen cursivering].

3. *Safe Harbour* is dood

Reële urgentie in de onderhandelingen met de VS kwam er pas (opnieuw) na de uitspraak van het Hofvan Justitie[1] op 6 oktober 2015 n.a.v. het beroep dat Max Schrems tegen de Ierse privacycommissie (in een procedure tegen *Facebook*, dat in Dublin zijn Europese hoofdzetel heeft) bij het Ierse Hooggerechtshof had ingesteld. Dat laatste stelde een prejudiciële vraag aan het Hof in Luxemburg, te weten of de Ierse privacycommissie (zoals deze had voorgehouden) gebonden was door de *Safe Harbour*-beschikking van de Commissie, in die mate dat niet meer in vraag zou kunnen worden gesteld dat het VS-dataprotectieregime adequaat was en ze dus geen onderzoek kon instellen naar de klacht die Schrems had ingediend. Die had in tegengestelde zin geargumenteerd n.a.v. de post-Snowden-vaststelling dat Face*book* in het PRISM-programma actief was, ondanks zelfcertificatie onder de *Safe Harbour*-principes.

Het Hof stelde o.m. vast dat '[h]et recht op eerbiediging van het privéleven, dat door artikel 7 van het Handvest en de kernwaarden die gemeen zijn aan de constitutionele tradities van de lidstaten wordt gewaarborgd, [...] elke gelding [zou] worden ontnomen wanneer overheden op aleatoire en algemene wijze toegang kunnen krijgen tot elektronische communicatie zonder dat hiervoor een objectieve rechtvaardiging hoeft te worden aangevoerd die berust op *overwegingen van nationale veiligheid of misdaadpreventie die specifiek met de betrokken personen verband houden*, en zonder te worden *omringd met passende en verifieerbare waarborgen*' [eigen cursivering] (paragraaf 34). Ook herinnerde het Hof, onder expliciete verwijzing naar het Dataretentiearrest van 8 april 2014[2] (waarbij het de Dataretentierichtlijn ongeldig had verklaard) en de onder de punten 54 en 55 daarvan aangehaalde arresten, aan zijn vaste rechtspraak dat 'een regeling van de Unie die een inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten met zich brengt [inzake het recht op eerbiediging van het recht op privacy respectievelijk dataprotectie] [...] *duidelijke en precieze* regels betreffende de draagwijdte en de toepassing van een maatregel [moet] bevatten [...]' (paragraaf 91). Nog onder verwijzing naar het Dataretentiearrest (en de onder punt 52 daarvan aangehaalde rechtspraak), stelde het Hof in aansluiting daarbij dat 'bovenal [...] de bescherming van het grondrecht op eerbiediging van het privéleven [vereist] dat de uitzonderingen op de bescherming van persoonsgegevens en de beperkingen ervan binnen de grenzen van het *strikt noodzakelijke* blijven' [eigen cursivering] (paragraaf 92), waarbij uiteraard als '*[n]iet beperkt tot het strikt noodzakelijke* een regeling is 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*'* [eigen cursivering] (paragraaf 93).

Met andere woorden: inzameling (bewaring), toegang en gebruik om redenen van nationale veiligheid, algemeen belang of rechtshandhaving behoeven dus *duidelijke en precieze* criteria en kunnen slechts wanneer *strikt noodzakelijk*, voor *specifieke doeleinden die strikt beperkt zijn*. Omdat de Commissie in haar *Safe-Harbour*-beschikking een dergelijke toetsing niet heeft doorgevoerd, verklaarde Het Hof deze dan ook ongeldig.

[1] HvJEU 6 oktober 2015, C-362/14, ECLI:EU:C:2015:650 (Maximilian Schrems v. Data Protection Commissioner).
[2] HvJEU 8 april 2014, C 293/12 en C 594/12, ECLI:EU:C:2014:238 (Digital Rights Ireland e.a.).

Met de Schrems-zaak heeft het Hof dus de vinger op de wonde gelegd: engagementen vanwege VS-bedrijven (via zelfcertificering onder de *Safe Harbour*-principes) bieden geen bescherming zolang het niet duidelijk is dat ondanks grootschalige interceptieprogramma's zoals PRISM het VS-privacyregime als adequaat kan worden beschouwd.

Gegeven de ongeldigverklaring van de *Safe-Harbour*-beschikking was een snel vervangingsinstrument evident noodzakelijk. De Europese Commissie (sinds november 2014 de Commissie Juncker, met Věra Jourová als commissaris voor justitie, fundamentele rechten en burgerschap, waaronder dataprotectie ressorteert, onder voogdij van supercommissaris (vice-voorzitter van de Commissie) *Frans* Timmermans) haastte zich om de gemoederen te bedaren. In verklaring op de dag van de uitspraak zelf nog erkende Timmermans dat het Hof de noodzaak had bevestigd *'of having robust data protection safeguards in place before transferring citizens' data'*. Hij voegde eraan toe dat de Commissie sinds haar *Safe Harbour*-mededeling al met de VS-autoriteiten aan het werk was '*to make data transfers* safer *for European citizens'* [eigen decursivering] en in het licht van de Schrems-uitspraak verder zou werken '*towards a* renewed and safe *framework for the transfer of personal data across the Atlantic*' [eigen decursivering].

4. Leve het privacyschild!

Op 29 februari 2016 kwam de Commissie dan met de langverwachte 'oplossing'. Ze lanceerde een nieuwe mededeling, getiteld 'Trans-Atlantische gegevensstromen: herstel van vertrouwen door solide waarborgen',[3] en hechtte er ineens – ter vervanging van haar ongeldig verklaarde *Safe Harbour*-beschikking – een ontwerp van adequatiebeslissing[4] van het VS-dataprotectieregime aan (met 7 bijlagen) voor gegevenstransfers onder de bescherming van een zogenaamd 'EU-VS-privacyschild'. Op de JBZ-Raad daags nadien toeterde Jourovà: *'Written assurances regarding the limitations on access to data by U.S. public authorities on national security grounds'*.

Alvorens het privacyschild op zijn merites te beoordelen, is het goed om weten dat het conceptueel erg sterk op de *Safe Harbour*-regeling gelijkt. De *Safe Harbour*-principes zijn hernoemd tot *privacy*principes, die de nieuwe basis moeten vormen voor datatransfers vanuit de EU naar organisaties – lees: bedrijven – in de VS die deze principes onderschrijven via zelfcertificering. Helemaal zoals voor de *Safe Harbour*-beschikking geldt er bovendien een uitzondering wanneer dat vereist is vanuit het oogpunt van *nationale veiligheid, algemeen belang of rechtshandhaving*.

Kernvraag is dan ook of de 'beperkingen' en 'waarborgen' die het privacyschild op dát stuk naar voren schuift – de *Safe Harbour*-regeling bevatte er géén – kunnen overtuigen. De krampachtige poging van de Europese Commissie om via haar mededeling en het eraan gehechte ontwerp van adequatiebeslissing aan te tonen dat de nieuwe regeling voldoet en de VS onder het privacyschild effectief een adequaat dataprotectieniveau vertonen, is ronduit pijnlijk. De hoogdagen van vorig Europees justitiecommissaris *Reding* lijken ver weg. Blijkbaar vergde het finaal toch te veel moed om van de VS een werkelijk engagement te eisen om niet meer in bulk en louter wanneer strikt noodzakelijk en proportioneel persoonsgegevens van EU-burgers of afkomstig uit de EU in te zamelen. Commissaris Jourová (en supercommissaris Timmermans) zijn jammerlijk gezwicht voor het dominant belang van goede trans-Atlantische handelsrelaties. Het mogelijk maken van trans-Atlantische persoonsge-

3 Trans-Atlantische gegevensstromen: herstel van vertrouwen door solide waarborgen. Mededeling van de Commissie aan het Europees Parlement en de Raad, COM(2016) 117 final, Brussel, 29 februari 2016.

4 Commission Implementing Decision of xxx pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.

gevenstransfers van bedrijven of vestigingen ervan in de EU naar bedrijven gevestigd in de VS is immers het primaire doel van het privacyschild. Té hard negotiëren is daarbij kennelijk geen optie geweest. Nochtans valt niet in te zien waarom commercieel persoonsgegevensverkeer zónder mogelijkheid om dat in bulk of disproportioneel voor inlichtingen- of politiedoeleinden te capteren een te hoge inzet voor de onderhandelingen zou zijn geweest. Bedrijven – ook de grote VS-spelers zoals *Google, Apple, Facebook* of *Microsoft* – zijn er finaal niet bij gebaat bij dat ze gegevens van hun Europese of andere gebruikers onvoldoende kunnen beschermen tegen overheidstoegang. Jammer dat ze dat zelf nog niet voldoende beseffen. Wellicht is het wachten tot gebruikers zich dreigen af te keren en de privacy-prijs die zíj betalen zich daadwerkelijk in winstvermindering voor de bedrijven in kwestie begint te vertalen.

In de tussentijd is het minste dat moet gebeuren, het doorprikken van het discours van de Europese Commissie in haar privacyschildmededeling en dito ontwerp-adequatiebeslissing. De 'beperkingen' en 'waarborgen' die het schild volgens de Commissie biedt tegen VS-datacollectie in functie van nationale veiligheid (door de inlichtingendiensten), algemeen belang of rechtshandhaving (door de politiediensten), zijn immers níet voldoende. Een gefocuste lezing en beperkte analyse volstaan om dat in te zien.

5. Beperkingen en waarborgen inzake datacollectie in functie van nationale veiligheid

a. Inzameling vs toegang en gebruik: één amalgaam

De analyse van de Commissie is misleidend, omdat ze het meermaals voorstelt alsof de 'beperkingen' waartoe de VS zich engageren zich op het stuk van 'toegang' en 'gebruik' (zie paragraaf 55 van de ontwerp-adequatiebeslissing: *'access and use'*) voor doeleinden van nationale veiligheid, algemeen belang of rechtshandhaving in het licht van het Unierecht volstaan om te kunnen gewagen van een adequate privacybescherming. Volgens EU-recht is er evenwel sprake van persoonsgegevensverwerking zodra er 'inzameling' plaatsvindt, ongeacht de latere 'toegang' ertoe of het later 'gebruik' ervan. Door systemisch de term 'toegang' te hanteren in plaats van 'inzameling' of het voor te stellen alsof beperkingen inzake 'toegang' in één beweging ook voldoende beperkingen inzake 'inzameling' inhouden, plaatst de Commissie de lezer op het verleerde been.

Voor zover nodig, volstaat het om het eerder aangehaalde Dataretentiearrest van het Hof van Justitie in herinnering te brengen. Het Hof maakte daarin immers – ten overvloede – duidelijk dat beperkingen noodzakelijk zijn zowel in de fase van de 'inzameling' van persoonsgegevens (in die context: retentie of bewaring door aanbieders van elektronische communicatiediensten van trafiekgegevens inzake vaste en mobiele telefonie, internettoegang, e-mail over het internet en internettelefonie) als in de fasen van de 'toegang' ertoe en het latere 'gebruik' ervan (in die context: door de bevoegde politiële en justitiële autoriteiten). De Commissie slaat dus een stap over, of probeert het minstens zo voor te stellen dat de privacyschild-beperkingen inzake 'toegang' en 'gebruik' op zich zouden kunnen volstaan om te kunnen gewagen van een adequate dataprotectie. Dat is valse retoriek. Ook op het stuk van de initiële 'inzameling' van persoonsgegevens door de bevoegde autoriteiten (*in casu*: de VS-inlichtingen- of -politiediensten) gelden strikte vereisten. Een van de redenen waarom het Hof immers de Dataretentierichtlijn ongeldig verklaarde (zie paragraaf 59) was omdat deze 'met name de bewaring niet [beperkte] tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit, of op

personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het voorkomen, opsporen of vervolgen van zware criminaliteit'. En toen ging het zelfs nog maar om de bewaring (en dus 'inzameling') door de aanbieders van elektronische communicatiediensten, en niet eens om de rechtstreekse 'inzameling' door inlichtingen- of politiediensten zelf, zoals in het kader van het privacyschild aan de orde is.

Daarnáást hekelde het Hof dat de Dataretentierichtlijn 'beperkingen [noch] objectieve criteria ter begrenzing van de *toegang* van de bevoegde nationale autoriteiten tot de gegevens en het latere *gebruik* ervan met het oog op het voorkomen, opsporen of strafrechtelijk vervolgen van inbreuken die, gelet op de omvang en de ernst van de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten, voldoende ernstig kunnen worden geacht om een dergelijke inmenging te rechtvaardigen [bevatte]' (paragraaf 60). En verder (in paragraaf 61) dat de Richtlijn evenmin de noodzakelijke 'materiële en procedurele voorwaarden [bevatte] betreffende de *toegang* van de bevoegde [...] autoriteiten tot de gegevens en het latere *gebruik* ervan', die volgens het Hof 'uitdrukkelijk' moesten gebonden zijn 'aan het doel, *nauwkeurig afgebakende* zware criminaliteit te voorkomen, op te sporen of strafrechtelijk te vervolgen', zodat aan de 'vereisten inzake noodzakelijkheid en evenredigheid' voor *toegang* niet zomaar kon worden voldaan door er een 'procedure en [...] voorwaarden [voor vast te stellen]'. Nog in verband met 'toegang' en 'gebruik' hekelde het Hof ten slotte (paragraaf 62) dat de Richtlijn 'geen objectieve criteria [bevatte] op basis waarvan het aantal personen dat de bewaarde gegevens mag *raadplegen* en vervolgens *gebruiken*, kan worden beperkt tot wat strikt noodzakelijk is voor de verwezenlijking van het nagestreefde doel' en dat 'bovenal [...] de *toegang* van de bevoegde [...] autoriteiten tot de bewaarde gegevens niet onderworpen [was] aan enige voorafgaande controle door een rechterlijke instantie of een onafhankelijke administratieve instantie waarvan de beslissing beoogt om de *toegang* tot de gegevens en het *gebruik* ervan te beperken tot wat strikt noodzakelijk is ter verwezenlijking van het nagestreefde doel en die uitspraak doet op een gemotiveerd verzoek van deze autoriteiten, ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten'.

Mutatis mutandis – in het kader van het privacyschild gaat het niet enkel om inzameling van, toegang tot en gebruik van persoonsgegevens door politiële en justitiële autoriteiten in het kader van zware criminaliteit, maar door inlichtingen- en politiediensten in het kader van nationale veiligheid, algemeen belang of rechtshandhaving – vallen uit het Dataretentiearrest dus zowel noodzakelijkheids- als proportionaliteitseisen af te leiden voor zowel het 'inzamelen' van gegevens enerzijds als de 'toegang' ertoe en het 'gebruik' ervan anderzijds.

Van de Commissie viel minstens te verwachten dat ze in haar privacyschild-mededeling zorgvuldig en systematisch, voor de onderscheiden fasen van 'inzameling' respectievelijk 'toegang en gebruik', de door de VS naar voren geschoven 'beperkingen' aan de EU-privacyeisen, zoals o.m. in het Dataretentiearrest geoperationaliseerd door het Hof, zou aftoetsen. Daarvan is manifest geen sprake. Inhoudelijk is het verder zo dat de garanties op het vlak van 'inzameling' kennelijk onvoldoende zijn. Inzameling in bulk blijft in een aantal scenario's immers gewoon mogelijk. Niet alleen kan dat – anders dan de Commissie het voorstelt – dus níet worden opgelost door de beperkingen die het privacyschild in huis heeft inzake 'toegang en gebruik'. De beperkingen op die laatste vlakken schieten eveneens te kort, want voldoen niet aan de eisen van noodzakelijkheid en proportionaliteit.

b. Inzameling in bulk blijft mogelijk

Op zich is het natuurlijk heuglijk nieuws (paragraaf 58 van de ontwerp-adequatiebeslissing) dat onder PPD-28 (de *Presidential Policy Directive* 28 van 17 januari 2014) inlichtingenope-

raties op het vlak van sigint (*Signals Intelligence* of het onderscheppen van elektronische communicatie) enkel nog maar mogen voor doelen van buitenlandse of contra-*intelligence* ter ondersteuning van *overheids*missies, en niet langer om VS-bedrijven commercieel te bevoordelen. Sigint voor industriële spionage of om VS-bedrijven orders te kunnen laten afsnoepen van Europese bedrijven, zoals o.m. bij Echelon het geval was gebleken, mag dus niet meer. Hoera.

Als bliksemafleider kan dit tellen. Na het Schrems-arrest is dát natuurlijk niet langer de inzet. De echte vraag is of de beperkingen aan gegevensinzameling voor overheidsdoelen op het stuk van nationale veiligheid, algemeen belang (anders dan economisch of in termen van competitievoordeel) of rechtshandhaving kunnen overtuigen. En dat doen ze niet – hoe hard de Commissie ook probeert dat te camoufleren. Aan vage engagementen vanwege de VS nochtans geen gebrek. Hieronder een bloemlezing.

Data-inzameling onder PPD-28 zal steeds *'as tailored as feasible'* zijn (paragraaf 58), en leden van de inlichtingengemeenschap [eigen decursivering] 'should *require that,* wherever practicable*, collection* should *be focused on specific foreign intelligence targets or topics* through the use of discriminants *(e.g. specific facilities, selection terms and identifiers).*' (paragraaf 59). Net iets te veel 'zou' om overtuigend te zijn. Ook '*wherever practicable*' is wel erg voorwaardelijk en vrijblijvend, en het loutere gebruik van 'discriminanten' waarborgt natuurlijk niet dat aan strikte noodzakelijkheids- of proportionaliteitseisen is voldaan – hooguit dat er niet zonder enige selectie sprake is van bulk-collectie. Bovendien erkennen de VS-engagementen vanwege het *Office of the Director of National Intelligence* (ODNI) zonder veel omhaal dat bulk-sigint in 'bepaalde' omstandigheden (die niet erg 'bepaald' blijken, zoals 'het identificeren van nieuwe of zich aandienende bedreigingen') toch nog zal plaatsvinden. De Commissie acht het blijkbaar voldoende geruststellend dat dit enkel mag gebeuren wanneer doelgerichte inzameling via het gebruik van discriminanten 'op basis van technische of operationele overwegingen' niet mogelijk wordt geacht. De erkenning door de Commissie zelf (handig weggemoffeld in voetnoot 31) dat het haalbaarheidsrapport dat de *Director of National Intelligence* aan president Obama had moeten aanleveren i.v.m. de mogelijkheid om software te ontwikkelen die het de inlichtingengemeenschap gemakkelijker moest maken '*eerder* aan doelgerichte dan aan bulk-inzameling' [eigen cursivering] te doen, concludeerde dat er géén software-gebaseerd alternatief is dat bulk-inzameling volledig kan vervangen, staat dat blijkbaar niet in de weg. De Commissie schaart zich vlotjes achter de inschatting van ODNI zelf dat bulk-inzameling dus niet de regel zal zijn (in plaats van de uitzondering) – alsof dat volstaat in het licht van de EU-eisen inzake inzameling. Geruststellend vindt de Commissie ook dat de beoordeling van wanneer meer gerichte inzameling technisch of operationeel 'niet haalbaar' wordt geacht niet aan de individuele willekeur van individuele personeelsleden van de inlichtingengemeenschap wordt overgelaten (paragraaf 60). Dat zou er nog moeten aan ontbreken. Een bijkomende 'waarborg' ziet de Commissie in het feit dat eventuele 'discriminanten' door hooggeplaatste beleidsmakers zullen worden bepaald, en regelmatig geëvalueerd (paragraaf 60). Helemaal overtuigd lijkt de Commissie wanneer de ODNI-engagementen duidelijk maken dat bulk-sigint-*gebruik* hoe dan ook 'beperkt' zal blijven tot een lijst van zes 'specifieke' nationale veiligheidsdoelen (infra, onder c). Beperkingen op het stuk van 'gebruik' vormen immers geen waarborgen op het stuk van 'inzameling'. Dat is nogal *basic* in het EU-privacyrecht. Slotsom, volgens de Europese Commissie, is dat, *'although not phrased in those legal terms'*, voldaan is aan de EU-vereisten inzake noodzakelijkheid en proportionaliteit (paragraaf 63): bulk-inzameling moet immers de uitzondering blijven, en wanneer ze toch plaatsvindt, gelden de zes 'strikte' *gebruiks*beperkingen. Anders geformuleerd: bulk-inzameling blijft mogelijk, en daarmee is geenszins voldaan aan de nauwe restricties die het EU-privacyrecht eist inzake de inza-

meling van gegevens. Je zou denken dat het Dataretentiearrest wat langer was blijven nazinderen, of dat we intussen allemaal wisten dat er sprake is van dataverwerking zodra er inzameling plaats vindt.

c. Toegang en gebruik voldoen niet aan strikte noodzakelijkheids- en proportionaliteitseisen

De zes 'specifieke' nationale veiligheidsdoelen waarvan hiervoor sprake en waartoe bulk-sigint-*gebruik* volgens de ODNI-engagementen 'beperkt' zal blijven, zijn de volgende (pagina 4, derde alinea van bijlage VI bij de ontwerp-adequatiebeslissing): *'detecting and countering certain activities of foreign powers, counterterrorism, counter-proliferation, cybersecurity, detecting and countering threats to U.S. or allied armed forces, and combating transnational criminal threats, including sanctions evasion'*. Behoorlijk voluntaristisch is degene die daar de specificiteit kan van inzien. Bovendien valt moeilijk in te zien dat het überhaupt om 'beperkingen' gaat, laat staan dat die al zouden kunnen overtuigen in het licht van de EU-eisen ter zake zoals geoperationaliseerd in het Dataprotectiearrest. Voor de Commissie is dat kennelijk muggenziften. In haar ontwerp-adequatiebeslissing probeert ze het overigens wel wat fraaier voor te stellen (paragraaf 61) door de zes vage doeleinden zelf níet te noemen, maar aan te voeren dat ze het mogelijk maken bedreigingen te detecteren en aan te pakken in de sfeer van spionage, terrorisme of massavernietigingswapens, tegen de strijdkrachten of tegen militair personeel, of in de sfeer van transnationale misdaad. Zulke voorstelling van zaken is niet langer eerbaar. Men zou van de Europese Commissie verwachten dat ze de privacy van de Europese burger beschermt en dat ze deze (via haar mededeling en ontwerp-adequatiebeslissing) correct voorlicht. Niet dat ze de Europese burger geringschat via holle en VS-vriendelijke retoriek en diens privacy blijft te grabbel gooien door de bulk-inzameling ervan voor vrijwel om het even welk VS-inlichtingendoel te faciliteren.

Alsof dat nog niet volstaat, moet het feit dat bovenstaande *gebruiks*-'beperkingen' ook gelden voor de *inzameling* van persoonsgegevens die via trans-Atlantische zeekabels verlopen – en dus buiten het grondgebied van de VS – ons volgens de Commissie helemaal geruststellen (paragraaf 62). Daarvoor geldt volledigheidshalve niet dat inzameling een verzoek vereist conform de FISA-wetgeving of door de FBI gedaan wordt op basis van een zogenaamde *National Security Letter*.

Dergelijk verzoek – zo beklemtoont de Commissie – is wel vereist wanneer de inlichtingengemeenschap informatie wil halen bij bedrijven op VS-territorium die 'zelfgecertificeerd' zijn onder het nieuwe privacyschild (paragraaf 65). Dergelijke 'toegang' – goed dat de term eindelijk eens in zijn correcte betekenis wordt gehanteerd – zou steeds heten doelgericht en beperkt te zijn, want het gebruik van specifieke selectietermen of -criteria vergen. Dat dit zelfs voor het PRISM-programma geldt, vindt de Commissie kennelijk een heuse opsteker: de informatie wordt immers geselecteerd aan de hand van individuele selectiecriteria zoals bv. emailadressen en telefoonnummers, en niet aan de hand van sleutelwoorden of namen van individuen (sic, paragraaf 68). De Commissie laat niet na om aan te stippen dat het volgens de *Civil Liberties Oversight Board* in de VS in voorkomend geval dus uitsluitend gaat om '*targeting specific [non-U.S.] persons about whom an individualised determination has been made*'. Voetnoot 72 verduidelijkt dat het verder loslaten van PRISM op VS-bedrijven onder het privacyschild derhalve niet neerkomt op ongerichte gegevensinzameling op grote schaal. Voilà. PRISM blijkt géén programma voor gegevensinzameling op grote schaal, of het is voldoende selectief om de toets met het Europese Privacyrecht te doorstaan. Kennelijk had de Commissie zich dus vergist wanneer ze in haar *Safe Harbour*-mededeling van eind november 2013 had geopperd dat het 'grootschalige karakter van deze programma's [...] tot gevolg [kon] hebben dat meer gegevens die in het kader van de veilige haven zijn doorgege-

ven, door de Amerikaanse autoriteiten [werden] geraadpleegd en verder verwerkt dan strikt noodzakelijk is voor en evenredig is met de bescherming van de nationale veiligheid, zoals de uitzondering waarin de veiligehavenbeschikking voorziet, bepaalt'. Bovendien, zo haalt de Commissie gretig aan, is er *empirisch bewijs* dat het aantal *targets* dat jaarlijks via PRISM wordt geaffecteerd 'relatief klein' is *'compared to the overall flow of data on the internet'* (randnummer 69). Bron daarvoor is het jaarrapport 2014 van ODSI zelf, waaruit inderdaad blijkt dat de PRISM-autorisatie onder FISA op 'slechts' 93.000 targets betrekking had. Niet grootschalig dus volgens de Commissie. Voeg daaraan de ODSI-garantie (in bijlage VI bij de ontwerp-adequatiebeslissing) toe dat bulk-inzameling slechts op een *'small proportion of the Internet'* plaats vindt, dit inclusief het capteren van gegevens op de trans-Atlantische kabels (randnummer 69), en iedereen is overtuigd.

Volgen nog een stuk of wat nietszeggende *bijkomende* garanties in de daaropvolgende paragrafen (70-74), zoals het feit dat het bv. niet volstaat dat sigint werd verzameld over de *'routine activities of a foreign person'* om die zomaar te kunnen verspreiden of blijvend bij te houden als daar niet ook andere intelligence-redenen voor zijn (randnummer 74). EU-burgers moeten dus niet vrezen: elektronische communicatie m.b.t. hun dagdagelijkse activiteiten worden niet permanent gestockeerd als daar geen goede redenen voor zijn.

Het laat de Commissie toe te besluiten (randnummer 75) dat er in de VS regels voorhanden zijn die zo ontworpen zijn dat 'elke interferentie voor doeleinden van nationale veiligheid met de fundamentele rechten van personen wiens gegevens onder het privacyschild van de EU naar de VS worden overgedragen beperkt blijft tot wat *strikt noodzakelijk* is om die legitieme doelstelling te realiseren' [eigen cursivering]. Daarmee moet de Europese burger het doen.

Wie dacht dat er na het arrest Schrems een reëel *issue* was met de commerciële doorgift van persoonsgegevens aan de VS omdat bedrijven daar die gegevens door de PRISM-filter moesten laten jagen, had het dus mis. Het Hof baseerde de ongeldigheid van het *Safe Harbour*-besluit van de Commissie technisch-juridisch gezien op het loutere feit dat deze laatste had verzuimd in dat besluit 'naar behoren met redenen omkleed [vast te stellen] dat [de VS], op grond van zijn nationale wetgeving of zijn internationale verbintenissen, daadwerkelijk waarborgen biedt voor een niveau van bescherming van de grondrechten dat in grote lijnen overeenkomt met dat binnen de rechtsorde van de Unie, zoals dat met name blijkt uit de voorafgaande punten van dit arrest' (randnummer 96), waarmee in essentie de verwijzing naar de inhoudelijke criteria van het Dataprotectiearrest werd bedoeld. De niet-vermelding door de Europese Commissie dat 'de VS daadwerkelijk op grond van hun nationale wetgeving of hun internationale verbintenissen 'waarborgen bieden' voor een passend beschermingsniveau' (randnummer 97) was voor het Hof dus het technisch-juridische breekpunt, 'zonder dat de veiligehavenbeginselen op hun inhoud [hoefden] te worden onderzocht' (randnummer 98). Alleen dat is kennelijk wat de Europese Commissie uit het arrest Schrems onthoudt, en reden waarom die Commissie meent ook te kunnen volstaan met een beargumenteerde vaststelling dat het VS-privacyregime voldoende waarborgen biedt. Met redenen omkleed is die vaststelling ontegenzeggelijk. Enkel is dat niet 'naar behoren' gebeurd – nochtans wel degelijk een van de eisen van het *Schrems*-arrest. De aangedragen argumentatie is selectief, vaak misleidend, soms gewoon vals. En moeite om een doorgedreven toetsing door te voeren aan de hand van de criteria die uit het Dataretentiearrest voortvloeien, getroost de Commissie zich zelfs niet, ook al verwijst het Hof er in de *Schrems*-zaak uitdrukkelijk naar terug.

d. Ombudspersoon

Uitweiden over de ultieme 'waarborg' die werd ingebouwd via de creatie van een Privacyschild-Ombudspersoon, is bepaald onnuttig. De ontwerp-adequatiebeslissing van de Commissie beklemtoont dat het een onafhankelijk mechanisme betreft, vrij van enige instructie vanwege de VS-inlichtingengemeenschap (randnummer 104). Gezien het om een vice-staatssecretaris van het ministerie van buitenlandse zaken van de VS gaat, dat in materies van nationale veiligheid toch niet bepaald afzijdig kan blijven, én er geen directe EU-betrokkenheid is in het Ombudsmechanisme, komt het Commissie-standpunt nogal gratuit voor. Wat er ook van zij, het enige waartoe de Ombudspersoon zich engageert, is om eventuele klachten te onderzoeken en te bevestigen dat het VS-recht, inclusief de hiervoor vermelde 'beperkingen' (die dus te kort schieten in het licht van het EU-recht), is nageleefd of dat, voor zover dat niet het geval zou blijken (wat in voorkomend geval overigens niet aan de klager wordt meegedeeld; of hij het voorwerp van een surveillancemaatregel heeft uitgemaakt, krijgt de klager evenmin te horen), daaraan is verholpen (randnummer 104 en punt 4.e van bijlage III bij de ontwerp-adequatiebeslissing). Bovendien wordt vakkundig de deur toegedaan voor eventuele klachten waarin – met reden dus – zou worden aangevoerd dat het privacyschild op zich niet conform zou zijn met de dataprotectievereisten van de EU. De brief van ODNI ter zake (bijlage III bij de ontwerp-adequatiebeslissing, punt 4.g) bepaalt laconiek dat het Ombudsmechanisme in voorkomend geval niet toepasselijk is. Niet meer dan een doekje voor het bloeden dus, die Ombudspersoon.

6. Beperkingen en waarborgen inzake datacollectie in functie van rechtshandhaving of algemeen belang

In haar ontwerp-adequatiebeslissing beoordeelt de Commissie ook de privacybeperkingen en -waarborgen die het VS-recht biedt in de *rechtshandhavings*sfeer. Ook op dat vlak is de conclusie – weinig verrasssend – dat het VS-dataprotectieniveau als adequaat moet worden beschouwd (randnummer 106). Zoeking en inbeslagneming door politiediensten vereist volgens het 4de amendement in principe een voorafgaand rechterlijk bevel op basis van *'probable cause'*. In bepaalde gevallen geldt het 4de amendement evenwel niet, omdat er voor sommige vormen van elektronische communicatie geen legitieme verwachting van privacy bestaat. In voorkomend geval is geen rechterlijk bevel nodig, en vallen de politiediensten terug op een 'redelijkheidstoets'. Die bestaat er eenvoudig in dat er een afweging wordt gemaakt tussen de mate waarin een zoekmaatregel inbreekt op de privacy van een individu en de mate waarin de maatregel nodig wordt geacht in functie van legitieme overheidsdoeleinden, zoals dat van rechtshandhaving (of een ander algemeen belang). De Europese Commissie concludeert vlotweg dat dit spoort met de 'idee' van ('*captures the idea of*') noodzakelijkheid en proportionaliteit in het EU-recht (randnummer 107). Ook het feit dat het 4de amendement überhaupt geen toepassing vindt op niet-VS-onderdanen buiten de VS is niet van aard de Commissie op andere gedachten te brengen. EU-burgers zouden indirect de bescherming genieten die de VS-bedrijven waar hun gegevens zijn gestockeerd, genieten. Op het feit dat die bescherming dus via een eenvoudige redelijkheidstoets aan kant kan worden gezet, waarbij de privacy van een bedrijf overigens niet noodzakelijk in het geding is omdat de politie in privégegevens van een klant geïnteresseerd is, wordt gemakshalve niet ingegaan. Er zijn volgens de Commissie overigens nog andere beschermingsmechanismen, zoals bv. richtlijnen van het ministerie van justitie die politiediensten enkel maar toegang tot privégegevens geven op gronden die de Commissie labelt als 'equivalent' aan noodzakelijkheid en proportionaliteit: zo stipuleren die immers dat de FBI zijn toevlucht

neemt tot de minst intrusieve maatregel (randnummer 108). Dat dit enkel iets zegt over de *subsidiariteit* in de aanwending van bepaalde onderzoeksmaatregelen, en niets te maken heeft met noodzakelijkheid of proportionaliteit, zal wel opnieuw muggenziften zijn. Ten slotte gaat de Commissie nog in op de praktijk van administratieve dwangbevelen (zoals destijds afgeleverd tegen de VS-hub van SWIFT). Die kunnen slechts in bepaalde gevallen en zijn onderworpen aan een onafhankelijke rechterlijke toetsing, zo valt er te lezen. Dat dit laatste slechts het geval is wanneer een bedrijf weigert spontaan uitvoering te geven aan een administratief dwangbevel en de overheid dus een beroep op de rechter moet doen om het bevel uitgevoerd te krijgen (randnummer 109), kan de pret niet bederven.

Ook wanneer administratieve dwangbevelen in functie van het *algemeen belang* worden afgeleverd, gelden overigens gelijkaardige beperkingen, zo leren we (randnummer 110). Administraties mogen immers alleen toegang bevelen tot gegevens die relevant zijn voor materies die onder hun bevoegdheid vallen – wat anders? – en moeten ook de genoemde redelijkheidstoets doorvoeren.

Genoeg reden voor de Commissie – veel woorden worden er niet meer aan verspild – om prompt tot een gelijklopende conclusie (randnummer 111) te komen als voor datacollectie in functie van nationale veiligheid. Het heet dat er in de VS regels voorhanden zijn die zo ontworpen zijn dat 'elke interferentie voor doeleinden van rechtshandhaving of ander algemeen belang met de fundamentele rechten van personen wiens gegevens onder het privacyschild van de EU naar de VS worden overgedragen beperkt blijft tot wat *strikt noodzakelijk* is om die legitieme doelstelling te realiseren' [eigen cursivering], en 'die een effectieve rechtsbescherming tegen zulke interferentie garanderen'.

Besluit

De ontwerp-adequatiebeslissing van de Europese Commissie is een vodje papier – meer niet. Onvoldoende, ongeloofwaardig, misleidend. Nochtans heeft de Commissie zich veel moeite getroost om uitvoerig uiteen te proberen zetten waarom we wél zouden moeten geloven dat de 'beperkingen' en 'waarborgen' die het VS-recht biedt sporen met de EU-vereisten van strikte noodzakelijkheid en proportionaliteit. De zaak Schrems heeft níets veranderd. Het privacyschild is een louter vervangingsinstrument voor de *Safe Harbour*-regeling. Die krijgen we gewoon opnieuw voorgezet in een nieuw jasje, zonder dat de situatie in de VS wezenlijk is veranderd. De havens van de VS-bedrijven zijn geen sikkepit veiliger geworden. PRISM en co blijft gewoon op de rails. Wat dachten we ook? Het enige nieuwe is dat de Commissie zich zo beijvert om een Trojaans paard te bouwen – want dat ís het privacyschild – en het tot voor de EU-poort te rollen. Aan de wakkere EU-burger om het niet binnen te halen. Als Europees privacycommissaris of –supercommissaris hield ik alvast de eer aan mezelf.

Referenties

G. Vermeulen (2004). Transatlantisch monsterverbond of verstandshuwelijk? Over het verschil tussen oorlog en juridische strijd tegen terreur en de versterkte politie- en justitiesamenwerking tussen EU en VS. *Panopticon*, 25(1), 90-107

E. De Busser, G. Vermeulen (2010). Towards a coherent EU policy on outgoing data transfers for use in criminal matters? The adequacy requirement and the framework decision on data protection in criminal matters. A transatlantic exercise in adequacy. In Cools *et al.* (Eds.) *EU and International Crime Control. Topical Issues*, Antwerp–Apeldoorn–Portland: Maklu, 95-122

E. De Busser (2009). *Data Protection in EU and US Criminal Cooperation*, Antwerp–Apeldoorn–Portland: Maklu, 474p.