Streep door gegevensdoorvoerregime voor de Verenigde Staten

1. 16 juli 2020 was de dag die je wist dat zou komen. Op die datum wees het EU Hof een arrest dat al jaren in de sterren geschreven stond. De uitspraak bevat dan ook weinig revolutionaire juridische interpretaties of complexe vraagstukken. Toch is het een uitspraak met zeer grote gevolgen, namelijk dat het doorvoeren van gegevens naar de Verenigde Staten lastiger wordt. Om deze uitspraak goed te begrijpen is een aanloopje nodig.

2. Alhoewel aanvankelijk primair opgericht en bedoeld als economisch samenwerkingsverband, waarin zonder barrières diensten, personen en goederen mogen worden doorgevoerd, tracht de EU al decennia ook ‘zachtere waarden’ zoals mensenrechtenbescherming te bieden. Dat lukt maar mondjesmaat, met als belangrijkste reden dat Europa al het Europees Verdrag voor de Rechten van de Mens en het Europees Hof voor de Rechten van de Mens heeft, waar vrijwel alle landen in Europa, en in ieder geval ook de EU-lidstaten, bij zijn aangesloten. Nog steeds is dat Hof leidend en dominant als het gaat om de bescherming van mensenrechten in Europa.

3. Er is echter een uitzondering, namelijk het recht op gegevensbescherming; op dat terrein neemt de EU het voortouw. Hier komen twee zaken bij elkaar: economie en mensenrechten. Het recht is dan ook een atypisch recht. De Algemene Verordening Gegevensbescherming van 2016, de opvolger van de Richtlijn bescherming persoonsgegevens uit 1995, houdt een beetje het midden tussen een marktreguleringsinstrument en een document dat beoogt mensenrechten te beschermen. De officiële doelstelling van de AVG, overigens in navolging van de Richtlijn uit 1995, is dan ook tweeërlei: aan de ene kant het beschermen van de rechten en vrijheden van burgers, aan de andere kant het mogelijk maken van het vrije verkeer in data binnen de EU (artikel 1 lid 2 AVG). Vrijwel alle bedrijven en overheidsinstanties zijn immers afhankelijk van de verwerking van persoonsgegevens. De AVG geeft in maar liefst 99 artikelen het kader waarbinnen deze organisaties moeten blijven om legitiem persoonsgegevens te mogen verwerken.

4. Ook anders dan bij de meeste andere mensenrechten is dat er een aparte toezichthouder is, die toeziet op de gegevensbeschermingsmarkt. In 1995, toen voor dit model werd gekozen, leek dat voor de hand liggend: net zoals de financiële sector, de medische sector en de telecomsector zou ook de gegevensverwerkingssector een eigen toezichthouder krijgen. Toen waren er immers nog maar een handvol overheidsinstellingen en bedrijven die op grote schaal gegevens verwerkten. Anno nu is dit model onhoudbaar. Aangezien vrijwel iedere burger, bedrijf en overheidsinstelling persoonsgegevens verwerkt is het onmogelijk voor een toezichthouder om daar goed zicht op te houden. Daarom is er in de AVG voor gekozen om het idee uit 1995 dat er een toezichthouder is die primair verantwoordelijk is voor de naleving en handhaving van de gegevensbeschermingsregels los te laten en te kiezen voor een secundaire rol van de Autoriteiten Persoonsgegevens van deze wereld. Met de inwerkingtreding van de AVG zijn bedrijven en overheidsinstellingen zelf primair verantwoordelijk voor het toezicht en naleving van deze regels binnen hun organisatie, onder meer door het aanstellen van een Data Protection Officer, het doen van Data Protection Impact Assessments en het bijhouden van registers van alle gegevensverwerkingen binnen hun organisatie, en is de Autoriteit Persoongsgevens een secundaire rol toegekend. Die controleert nu met name of organisaties hun interne toezicht op orde hebben.

5. De EU heeft een unieke positie ten aanzien van het recht op gegevensbescherming. In alle andere delen van de wereld en zelfs binnen de Raad van Europa kent men geen afzonderlijk

recht op gegevensbescherming, maar wordt het gezien als onderdeel van het recht op privacy, namelijk de *informational privacy*. De EU heeft een apart recht gecreëerd: het recht op gegevensbescherming, dat losstaat van het recht op privacy. Alle gegevens die aan een persoon zijn gerelateerd, of die nu gevoelig zijn of niet, vallen onder dit regime, dus ook een zin als 'Rutte heeft leuk haar'. De reikwijdte van dit recht is daarmee ongekend en het uitgangspunt van het fundamentele recht op gegevensbescherming, zoals vervat in artikel 8 van het Handvest, is dan ook niet, zoals bij andere mensenrechten, dat een inperking op een mensenrecht is verboden, tenzij is voldaan aan alle beperkingsvoorwaarden, maar dat het verwerken van persoonsgegevens legitiem is, mits wordt voldaan aan een aantal randvoorwaarden.

6. De achtergrond van dit recht was dat een aantal landen binnen de EU uiteenlopende regels voor het verwerken van persoonsgegevens kenden. Dit belemmerde het vrije verkeer van persoonsgegevens, omdat bijvoorbeeld een Italiaans bedrijf dat ook vestigingen had in vijf andere EU-landen, aan zes verschillende regimes moest voldoen, met soms conflicterende regels en verplichtingen. Om een einde te maken aan deze barrières werd afgesproken om het gegevensbeschermingsniveau gelijk te trekken. Overal zou een hoog beschermingsniveau gelden, waardoor in ieder geval binnen de EU alle gegevens vrijelijk kon worden doorgevoerd. Zo was de gedachte in 1995 althans. Er waren twee hoofdzakelijke obstakels om deze gedacht in de praktijk te brengen.

7. Enerzijds waren de regels uit 1995 vervat in een richtlijn, wat tot gevolg had dat landen toch weer elk zo hun eigen interpretatie van de regels hadden. Sommige landen interpreteerden het kader een stuk soepelere dan anderen. De handhaving van de regels was belegd bij nationale handhavende organisaties, terwijl sommige landen meer geld en middelen aan deze organisaties ter beschikking stelden dan anderen. Het gevolg was dat sommige landen een lage regel- en handhavingsdruk kenden, zoals Ierland, en dat grote internationale ondernemingen zich daar vestigden (waarbij overigens ook de belastingdruk een rol speelt). Zo ook Facebook. Zo kon formeel aan de EU gegevensbeschermingsregels worden voldaan, terwijl de regels zo minimaal mogelijk werden geïnterpreteerd en grensgevallen nauwelijks werden gecontroleerd (zie verder: Kuner, C. (2017). Reality and illusion in EU data transfer regulation post Schrems. *German Law Journal*, *18*(4), 881-918).

8. Anderzijds is de EU het enige blok ter wereld dat het gegevensbeschermingsrecht als apart fundamenteel recht kent. Gegevens die de EU verlaten worden dan ook in principe niet in gelijke mate beschermd als binnen de EU. Daarom werd bedacht dat persoonsgegevens over EU-burgers de EU slechts mochten verlaten als min of meer hetzelfde beschermingsregime als in de EU werd gehandhaafd in de ontvangende niet EU-staat. Dat kan allereerst doordat een land als zodanig wetgeving aannam die gelijk was aan de EU-regels, waarbij het idee was dat net zoals de VS lange tijd zijn intellectueel eigendomsrechtregime had geëxporteerd naar landen over de hele wereld, als onderdeel van handelsverdragen, dat de EU als economisch machtsblok kon afdwingen dat derde landen haar gegevensbeschermingsregime zou overnemen. Dat bleek maar een beperkt succes. Zo'n dozijn gebieden hebben inmiddels een zogenoemde 'adequacy decision' van de Commissie bemachtigd (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en). Een andere mogelijkheid is dat bedrijven of organisaties in de landen buiten de EU zich contractueel vastlegden op het naleven van de EU gegevensbeschermingsregels. Ten aanzien van de naleving van dit soort contracten, waarvoor binnen de EU modelcontracten zijn ontwikkeld, hebben de nationale handhavende organisaties een leidende rol. Dit regime werkt redelijk, maar er was een knelpunt: de

Verenigde Staten. De VS voldoen niet aan de EU gegevensbeschermingsregels als geheel maar zijn een te groot handelsblok om buiten te sluiten. Als handhavende organisaties werkelijke alle bedrijven en organisaties die zaken doen in de EU of waarmee bedrijven in de EU zaken doen zouden controleren op goede contractuele afspraken en naleving van die afspraken, dan zou dat veel geld en tijd kosten en hoogstwaarschijnlijk een flinke barrière voor de handelsrelatie tussen beide blokken opleveren.

9. Voor beide problemen werd een oplossing gevonden. De AVG, die de Richtlijn uit 1995 verving, is een Verordening en heeft dus directe werking. De regels binnen de EU werden daarmee, op enkele uitzonderingen na waar de AVG lidstaten ruimte laat om een eigen interpretatie te kiezen, geharmoniseerd. Landen worden er door de AVG toe verplicht deze organisaties goed te equiperen en de organisaties kunnen nu binnen een samenwerkingsverband invloed uitoefenen op het beleid en de aanpak van een nationale autoriteit als die toezicht houdt op een organisatie die in dat land is gevestigd, maar aan grensoverschrijdende gegevensverwerking doet en daarmee de burgers in andere EU-landen raakt. De AVG is ook direct van toepassing op bedrijven die in de EU zaken doen (Bradford, A. (2012). The brussels effect. *Nw. UL Rev.*, *107*, 1).

10. Anderzijds verzon de Europese Commissie al voor het de inwerkingtreding van de AVG een list: er werd een soort tussenregime gecreëerd dat het midden hield tussen een adequacy decision en een model waarin alle Amerikaanse organisaties zelf contractuele afspraken moeten maken met alle EU-organisaties waarmee zij zaken doen. Er werd een model van zelfcertificering in het leven geroepen, waarbij Amerikaanse organisaties zichzelf konden aanmelden en verklaren dat zij aan de EU gegevensbeschermingsregels voldeden. Een opmerkelijke oplossing, omdat het gevolg uiteraard was dat veel organisaties simpelweg claimden de regels te volgen maar dat niet deden en de Amerikaanse overheid en met name de inlichtingendiensten zeer verregaande bevoegdheden hebben om data van in de VS gebaseerde organisaties op te eisen, zonder dat EU-burgers hun rechten kunnen claimen (Decision 2000/520/EC).

11. Daarom diende Max Schrems, toen nog rechtenstudent te Oostenrijk, een klacht in over dit regime, dat hij bij wijze van voorbeeld indiende tegen Facebook. Na wat geheen-en-weer tussen het bedrijf, de Ierse Data Protection Authority en de Ierse rechter besloot een rechtbank prejudiciële vragen te stellen aan het EU Hof van Justitie. Dat kwam in 2015 tot een zeer verregaande conclusie: het regime zoals door de Commissie ingesteld was ongeldig en ondeugdelijk (CLI:EU:C:2015:650, Judgment of the Court (Grand Chamber) of 6 October 2015). Wat deed de Europese Commissie in reactie daarop? Gewoon eenzelfde soort regime instellen, met wat minimale en kosmetische aanpassingen (Uitvoeringsverordening (EU) 2016/1250). Wat deed Schrems? Weer een klacht indienden. En wat deed het Hof van Justitie toen er wederom prejudiciële vragen werden gesteld? Wederom het regime ongeldig en ondeugdelijk verklaren in het voorliggende arrest, min of meer op dezelfde punten als het eerste regime ongeldig was verklaard. Het Hof oordeelt dat met name het surveillanceprogramma door Amerikaanse inlichtingendiensten niet voldoet aan de standaarden van de EU. Dat komt onder meer omdat er geen toets van proportionaliteit en subsidiariteit wordt opgelegd aan het gebruik van bevoegdheden door deze diensten. Ook is de Amerikaanse wetgeving volgens het Hof niet voldoende helder en geeft het niet voldoende precies aan welke bevoegdheden onder welke voorwaarden mogen worden ingezet en wat de grenzen daar aan zijn. Burgers kunnen zich bovendien maar in zeer beperkte mate beroepen op hun rechten en Amerikaanse rechters hebben maar beperkte bevoegdheden om de

surveillanceactiviteiten van inlichtingendiensten onder de loep te nemen. Ook de ombudsmanfunctie is niet toereikend. Een strikte lezing van dit arrest zou met zich brengen dat er geen gegevens meer mogen worden doorgevoerd naar de VS, totdat het land zijn regime heeft aangepast. In de VS gebaseerde organisaties kunnen zich immers maar moeilijk onttrekken aan de bevoegdheid van inlichtingendiensten om toegang te claimen tot de door hen bewaarde persoonsgegevens (over Amerikaanse, Europese en andere burgers).

12. Daarnaast is nog een handvol andere punten in deze zaak van belang. Zo is er een besluit van de Commissie ten aanzien van de modelcontracten (**Decision 2010/87/EU)**. Als organisaties deze standaardcontracten implementeren en ondertekenen, dan worden ze geacht een aan de AVG-gelijkwaardig beschermingsniveau te hebben geïmplementeerd. Na de eerste Schrems uitspraak is dat besluit nog wat verder aangepast een aangescherpt. Is dat besluit ook in strijd met artikelen 7 en 8 uit het Handvest? Nee, dixit het Hof. In het modelcontract zegt de contractant toe zich aan alle geldende wettelijke bepalingen te zullen houden en daartoe de nodige maatregelen te treffen. De geldende wettelijke bepalingen omvatten ook de bepalingen uit de AVG. Als er binnen een land geen goede gegevensbeschermingsbepalingen zijn, dan zal de organisatie dus zelf maatregelen moeten treffen. Als dat niet lukt of kan lukken, omdat het rechtsstelsel in een derde land verplichtingen aan een organisatie oplegt die in strijd zijn met de AVG, dan moet deze organisatie dat melden aan de in de EU-gevestigde partner. Die moet daarop de doorvoer stoppen. Daarop moeten alle doorgevoerde gegevens worden vernietigd. Ook de handhavende organisatie van het land waarin de in de EU-gevestigde organisatie zetelt mag in zulke gevallen verordonneren dat de doorvoer moet stoppen.

13. Wellicht nog het meest interessant in dit arrest is de vraag naar de rol van de nationale handhavende organisatie. Die heeft de bevoegdheid om gegevensdoorvoer naar landen buiten de EU stop te zetten als die niet aan de AVG voldoet. Maar is die organisatie daartoe ook verplicht als zij meent dat niet wordt voldaan aan het EU gegevensbeschermingsniveau? Ja, zegt het Hof, tenminste als het duidelijk is dat andere maatregelen, zoals waarschuwingen, aanbevelingen of onderzoeken geen soelaas zullen bieden. Een handhavende organisatie mag er derhalve niet voor kiezen niet corrigerend op te treden. Of dit alleen voor gegevensdoorvoer naar derden landen geldt, of meer in het algemeen betekent dat handhavende organisaties de plicht, en niet de bevoegdheid, hebben om op te blijkt niet uit het arrest of de AVG. Dat laatste zou een verregaande inperking van de beleidsruimte van handhavende organisaties met zich brengen.

14. Mag de Autoriteit ook oordelen dat de standaardcontractbepalingen zelf en/of een eventuele adequaatheidsbeslissing van de Commissie ongeldig is? Nee, daartoe heeft het geen bevoegdheid. Als het een klacht hieromtrent binnenkrijgt van een datasubject, dan moet het deze klacht onderzoeken en als het daartoe aanleiding ziet, beroep kunnen instellen bij een nationale rechter, die vervolgens prejudiciële vragen kan stellen. Interessant is dat het Hof hiermee lijkt te suggereren dat lidstaten de plicht hebben om in hun wettelijk regime mogelijk te maken dat handhavende organisaties klachten voor de rechter kunnen brengen.

15. Hoe moet dan worden beoordeeld of er een passend gegevensbeschermingsniveau is in een derde land of binnen een organisatie gevestigd in een derde land? Daarover is het Hof niet zo duidelijk. Er moeten passende waarborgen zijn, afdwingbare rechten en doeltreffende rechtsmiddelen. Een groot deel hangt dus samen met de rechten van burgers en of die rechten effectief kunnen worden ingeroepen in dat derde land.

16. Tot slot: is de AVG überhaupt wel van toepassing in deze zaak? De AVG zondert immers verwerking in het kader van nationale veiligheid uit (artikel 2 lid 2 AVG), zoals activiteiten van inlichtingendiensten in het kader van terrorismebestrijding, wat geldt voor het gehele EU-recht. Toch is het AVG-regime van toepassing zegt het Hof, omdat in casu gegevens werden doorgevoerd door een commerciële partij. Dat die later in een derde land eventueel kunnen worden ingezien en verwerkt door inlichtingendiensten is secundair. De uitzonderingsgronden op het materieel toepassingsgebied van de AVG die zijn vervat in artikel 2 lid 2 moeten beperkt worden uitgelegd. Dat is interessant, omdat van Amerikaanse zijde vaak werd gesteld dat het EU Hof met de eerdere Schrems uitspraak, in feite met twee maten meet. Stel gegevens worden van Nederland naar Hongarije doorgevoerd en de Hongaarse inlichtingendiensten hebben zeer grote bevoegdheden om die gegevens in te zien. Zou het Hof in zo'n geval de doorvoer verbieden naar Hongarije omdat de inlichtingendiensten in dat land te grote bevoegdheden hebben? Vermoedelijk niet, maar in het geval het dat wel zou doen, gaat het Hof dan niet zijn boekje te buiten? Het EU Hof blijft onverstoord en oordeelt wederom langs de lijn waarop het eerder deed.

Bart van der Sloot
Privacy-goeroe, Universiteit Tilburg