Kroniek Privacy en Gegevensbescherming

In deze kroniek over de ontwikkelingen in het privacy- en gegevensbeschermingsrecht staan centraal een aantal uitspraken van het Europees Hof voor de Rechten van de Mens en het Europees Hof van Justitie van de afgelopen twee jaar en de aanstondse Algemene Verordening Gegevensbescherming die op termijn de huidige Richtlijn bescherming persoonsgegevens zal vervangen. De kroniek ziet dus met name op de Europese ontwikkelingen, in het bijzonder ten aanzien van wat ook wel wordt genoemd de 'informationele privacy'. Omdat de ontwikkelingen op dit gebied nogal talrijk zijn, is een keuze in onderwerpen gemaakt.

1. Introductie

Er is thans veel te doen rondom het thema van privacy en gegevensbescherming in Nederland. Zo heeft de Wetenschappelijke Raad voor Regeringsbeleid onlangs een advies aan de Nederlandse regering overhandigd over de regulering van Big Data, met name in verband met het gebruik daarvan door politie en inlichtingendiensten.[1] Ook is er al langer sprake van een mogelijke herziening[2] van de Wet op de Inlichtingen- en Veiligheidsdiensten,[3] waarover vrijwel voortdurend discussie is, met name over de vraag in hoeverre er gebruik kan worden gemaakt van zogenoemde sleepnetconstructies, waarbij de gegevens van vele miljoenen onschuldige burgers kunnen worden verzameld. Daarnaast is er een nieuwe wet aangenomen omtrent het hergebruik van overheidsinformatie[4] en is er al jaren discussie over de vraag in hoeverre oude bepalingen in de Grondwet, bijvoorbeeld ten aanzien van het 'briefgeheim', het 'lichaam' en de 'woning', allemaal nogal analoge formuleringen, geschikt kunnen worden gemaakt voor het digitale tijdperk.[5] Tot slot zijn er tal van relevante rechtszaken gewezen, bijvoorbeeld over de Paspoortwet,[6] de samenwerking tussen Nederlandse en buitenlandse inlichtingendiensten[7] en de mogelijkheid om advocaten af te tappen.[8]

Toch is er in dit stuk voor gekozen om met name de Europese ontwikkelingen onder de loep te nemen, omdat deze uiteindelijk bepalender zullen zijn voor zowel de Europese en internationale alsmede de Nederlandse ontwikkeling op het gebied van privacy en gegevensbescherming. Ook daar is evenwel zo veel te doen over dit thema dat er is gekozen om een selectie te maken, om zo een aantal ontwikkelingen uitvoeriger te kunnen bespreken, in plaats van meer zaken kort aan te stippen. Een keuze daarin is gemaakt op basis van hun

[1] WRR, Big Data in een vrije en veilige samenleving <http://www.wrr.nl/fileadmin/nl/publicaties/PDF-Rapporten/rapport_95_Big_Data_in_een_vrije_en_veilige_samenleving.pdf>.
[2] https://www.internetconsultatie.nl/wiv
[3] Wet van 7 februari 2002, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 2002)
[4] Wet hergebruik overheidsinformatie, Stb. 2015, 271. B. van der Sloot, 'Van openbaarheid naar hergebruik van overheidsinformatie Of een vaarwel aan het sociaal contract', <http://www.ivir.nl/publicaties/download/1699>.
[5] WODC, 'Bescherming van grondrechten in het digitale tijdperk: Verslag van een internationale discussie over concept-voorstellen van de Commissie Grondrechten in het digitale tijdperk', <https://www.wodc.nl/images/99.130-volledige-tekst_tcm44-583316.pdf>.
[6] Hoge Raad, ECLI:NL:HR:2015:1296, 22 mei 2015.
[7] Rechtbank Den Haag, ECLI:NL:RBDHA:2014:8966, 23 juli 2014.
[8] Gerechtshof Den Haag, ECLI:NL:GHDHA:2015:2881, 27 oktober 2015.

invloed, de mate waarin zij discussie hebben opgeroepen in de literatuur en hun mogelijke revolutionaire of vernieuwende karakter. Deze selectie is uiteraard subjectief.

De volgende onderwerpen zullen aan bod komen. Ten eerste heeft het EHRM in een aantal zaken, met name *Zakharov t. Rusland*[9] en *Szabó en Vissy t. Hongarije*,[10] over 'mass surveillance' gesteld dat het zogenoemde *in abstracto* claims zal ontvangen, dat wil zeggen, zaken over de legitimiteit en legaliteit van wetten als zodanig, zonder dat die noodzakelijkerwijs een impact hoeven te hebben gehad op de klagers (paragraaf 2).[11] Ten tweede is het Hof van Justitie in de loop der jaren steeds bepalender en activistischer geworden op het terrein van privacy en gegevensbescherming; dit wordt geïllustreerd aan de hand van een bespreking van twee zaken, namelijk *Digital Rights Ireland*[12] en *Google Spain*[13] (paragraaf 3). Ten derde is er flink wat te doen over de transnationale gegevensstromen, met name van en naar de Verenigde Staten; de aanleiding hiervoor is de zaak *Schrems*[14] (paragraaf 4).[15] Ten vierde wordt er al langer geageerd tegen de vaak onbegrijpelijke wijze waarop het HvJ en het EHRM tot hun oordelen komen en tegen de methode van 'balancing', het afwegen van verschillende belangen, die vaak wordt toegepast.[16] Deze al oudere kritiek zwelt de laatste tijd weer aan en niet ten onrechte, zo zal worden geïllustreerd aan de hand van de zaken *Coty*[17] en *Delfi*[18] (paragraaf 5).[19] Ten vijfde en tot slot wordt de huidige Richtlijn bescherming *persoonsgegevens*,[20] waarop ook de Nederlandse Wet bescherming persoonsgegevens is gebaseerd,[21] op termijn vervangen door een Algemene Verordening Persoonsgegevens, die kort zal worden toegelicht (paragraaf 6).

2. Het EHRM als constitutioneel hof: *Zakharov t. Rusland* en *Szabó en Vissy t. Hongarije*

Het Europees Hof voor de Rechten van de Mens heeft onlangs twee revolutionaire zaken gewezen ten aanzien van artikel 8 EVRM, namelijk Zakharov t. Rusland en Szabó en Vissy t. Hongarije. Het revolutionaire karakter behoeft enige inleiding. Aanvankelijk was het EVRM vooral gestoeld op het idee van de bescherming van algemene belangen, met name gericht op het voorkomen van machtsmisbruik door de overheid. Een voorbeeld hiervan is bijvoorbeeld het stelselmatig discrimineren van grote categorieën in de samenleving, het ontzeggen van vrijheden van bepaalde bevolkingsgroepen om het op grote schaal bespioneren van de bevolking, zoals onder meer gebeurde in de diverse fascistische en communistische regimes tijdens de Tweede Wereldoorlog en ook later nog door bijvoorbeeld de Stasi in de DDR. Hoe dan ook ging het om grote maatschappelijke misstanden en problemen en niet

[9] ECtHR, Roman Zakharov v. Russia, appl.no. 47143/06, 04 december 2015.
[10] ECtHR, Szabó and Vissy v. Hungary, appl.no. 37138/14, 12 januari 2016.
[11] Dit is deels gebaseerd op: B. van der Sloot, 'Editorial', EDPL 2016-1.
[12] HvJ, ECLI:EU:C:2014:238, 8 april 2014.
[13] HvJ, ECLI:EU:C:2014:317, 13 mei 2014.
[14] HvJ, ECLI:EU:C:2015:650, 6 oktober 2015
[15] Dit is deels gebaseerd op: B. van der Sloot, 'Annotatie Coty', European Human Rights Cases, 2015-10, nr. 188.
[16] Zie verder: B. van der Sloot, 'The Practical and Theoretical Problems with 'balancing': Delfi, Coty and the redundancy of the human rights framework', Maastricht Journal of European and Comparative Law, 3 2016.
[17] HvJ, ECLI:EU:C:2015:485, 16 juli 2015.
[18] ECtHR, Delfi AS v. Estonia, appl.no. 64569/09, 16 juni 2015.
[19] Dit is gebaseerd op: B. van der Sloot, 'Machtsstrijd over persoonsgegevens: De zaak Schrems v. Data Protection Commissioner van het Europees Hof van Justitie', Ars Aequi, april, 2016.
[20] 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. Publicatieblad Nr. L 281 van 23/11/1995 blz. 0031 – 0050.
[21] Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens)

over de particuliere problemen van individuele burgers. De bedoeling was dan ook dat er met name interstatelijke klachten zouden komen over dergelijke misstanden, waarbij bijvoorbeeld Nederland een klacht tegen het Verenigd Koninkrijk kon indienen. Na lang onderhandelen werd ook een individueel klachtrecht opgenomen in het Verdrag, namelijk voor natuurlijke personen, groepen en rechtspersonen (niet zijnde overheidsorganisaties). Daarbij moeten echter drie zaken worden opgemerkt. Ten eerste betreft het hier niet slechts natuurlijke personen, maar ook groepen en rechtspersonen die een klacht mogen indienden; de gedachte hierachter was dat ook de individuele klachten met name betrekking zouden hebben op maatschappelijke misstanden, waartegen een individu, een groep of een rechtspersoon in het geweer zou kunnen komen. Ten tweede kon er ten aanzien van dit klachtenrecht een voorbehoud worden gemaakt door landen, almede ten aanzien van de bevoegdheden van het EHRM. Ten derde en tot slot, in tegenstelling tot interstatelijke klachten, hadden individuele klagers slechts de bevoegdheid om een zaak in te dienen bij de Europese Commissie voor de Rechten van de Mens, die over de ontvankelijkheid van zaken besliste en niet bij het Europees Hof voor de Rechten van de Mens, dat oordeelt over de vraag of er een schending van een mensenrecht is geweest of niet. Zelfs als een zaak ontvankelijk was verklaard door de Commissie kon deze alleen worden voorgelegd aan het Hof door een lidstaat of door de Commissie. Het individuele klachtenrecht was derhalve zeer beperkt.

Dit beeld heeft zich langzamerhand gewijzigd. Klagers hebben nu bijvoorbeeld wel directe toegang tot het Hof. Daarnaast heeft het EHRM geoordeeld dat groepen niet mogen klagen over een schending van een mensenrecht; alleen natuurlijke personen die direct en individueel zijn getroffen mogen hun klachten bundelen, dit in expliciete tegenspraak met de bedoeling van de opstellers van het Verdrag. Bovendien heeft het EHRM geoordeeld dat rechtspersonen in principe niet mogen klagen over een schending van het recht op privacy, omdat dit recht met name persoonlijke en individuele belangen beschermt. Alhoewel hieromtrent recentelijk een iets soepeler houding valt te ontwaren, blijft het klachtrecht van rechtspersonen ten aanzien van artikel 8 EVRM zeer beperkt. Ook de interstatelijke klachten spelen in de praktijk nauwelijks een rol van betekenis. Tot slot moet worden bedacht dat het EHRM ten aanzien van de klachten van natuurlijke personen met betrekking tot het recht op privacy heeft gesteld dat deze in principe alleen ontvankelijk zullen worden verklaard als een klager kan aantonen direct, individueel en aanmerkelijk te zijn geschaad in zijn belangen. Daaruit volgt onder meer dat *in abstracto* claims (ten aanzien van de legitimiteit en noodzakelijkheid van een wet of beleid als zodanig, zonder dat deze is toegepast of een impact heeft gehad op de klager) niet ontvankelijk zullen worden verklaard. Dit geldt ook voor *actio popularis* of class actions (zaken die aanhangig worden gemaakt door klagers die willen opkomen voor een algemener, maatschappelijk belang), voor hypothetische klachten (over schade die zich zou kunnen hebben gematerialiseerd, maar waarover de klager geen zekerheid heeft), klachten ten aanzien van mogelijke toekomstige schade en ten aanzien van zaken met een zeer minimale impact op de individuele belangen van de klager.

Deze nadruk op klachten van natuurlijke personen die direct en individueel getroffen moeten zijn heeft een aantal duidelijke nadelen. Zo gaat het al snel om vrij futiele klachten over bijvoorbeeld de vraag of iemand een ander een poephoofd mag noemen op een blog, of dit niet moet worden gezien als een schending van diens recht op reputatie als beschermd door artikel 8 EVRM en of iemand anders een poephoofd noemen, of zelfs een blog faciliteren waarop andere elkaar voor poephoofd kunnen uitmaken, niet onder de vrijheid van meningsuiting moet vallen (zie paragraaf 5). Ook komt het EHRM met zijn eigen criteria in de knel in zaken waar het gaat om grootschalige misstanden. Een voorbeeld hiervan zijn de ‘mass surveillance’-wetten, die thans in veel landen worden aangenomen en die inlichtingendiensten en soms ook de politie verregaande bevoegdheden toekennen om via sleepnetconstructies over vrijwel alle burgers data te verzamelen. Het probleem daarbij is

tweeërlei. Ten eerste zijn deze overheidsdiensten vaak niet open over hun exacte werkwijze, zodat het voor individuele burgers onduidelijk blijft of en zo ja, in hoeverre zij zijn meegenomen in het sleepnet. Ten tweede, zelfs als zij dat wel zouden weten, blijft de individuele schade die hieruit volgt vaak lastig te duiden. Welke impact heeft bijvoorbeeld de grootschalige gegevensverzameling van de NSA gehad op het leven van een gewone Europese of Amerikaanse burger? Om dit probleem te omzeilen is het Hof al vanaf 1978 (de Klass zaak) bereid geweest om het slachtoffer-vereiste soepeler te interpreteren in dit soort zaken. Met name in de laatste jaren is het Hof hier steeds ruimer in geworden. Het punt was echter dat het Hof nooit expliciet heeft willen toegegeven dat het in dit soort zaken moet en wil werken met een andere benadering van het schadevereiste. Dat is nu in de twee voorgenoemde zaken veranderd; daarin heeft het Hof expliciet aangegeven dat het in uitzonderlijke zaken ook *in abstracto* claims zal ontvangen.

In de Zakharov zaak stelde het EHRM bijvoorbeeld dat 'the Court accepts that an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions are satisfied. Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies. As the Court underlined in *Kennedy*, where the domestic system does not afford an effective remedy to the person who suspects that he or she was subjected to secret surveillance, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such circumstances the menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8. There is therefore a greater need for scrutiny by the Court and an exception to the rule, which denies individuals the right to challenge a law *in abstracto,* is justified. In such cases the individual does not need to demonstrate the existence of any risk that secret surveillance measures were applied to him. By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures.'[22]

In de zaak Zakharov, beoordeelde het EHRM in algemene zin of de Russische wet die de wettelijke basis vormde voor de mass surveillance activiteiten door overheidsdiensten voldeed aan de minimum voorwaarden van rechtsstatelijkheid. Onder andere beoordeelde het de toegankelijkheid van de nationale wetten, het toepassingsgebied van de maatregelen van de geheime diensten, de duur van de toezichtsmaatregelen, de te volgen procedures voor het opslaan, de toegang tot, het onderzoeken, het gebruik, de communicatie en het vernietigen van de onderschepte gegevens, de autorisatie van de geheime surveillance maatregelen, het toezicht op de uitvoering van de geheime toezichtmaatregelen, de kennisgeving van geheime toezichtsmaatregelen en de beschikbare rechtsmiddelen. Het EHRM concludeerde dat de wettelijke bepalingen met betrekking tot het aftappen van communicatie niet voorzagen in adequate en effectieve waarborgen tegen willekeur en het risico van machtsmisbruik, dat

[22] Zakharov, paragraaf 171.

inherent is aan elk systeem van mass surveillance, en dat bijzonder hoog is in een systeem waarbij de geheime dienst en de politie, met technische middelen, zich direct toegang kunnen verschaffen tot alle mobiele communicatie.

In het bijzonder benadrukt het EHRM dat de omstandigheden waarin overheden bevoegd waren hun toevlucht te nemen tot geheime surveillance maatregelen niet waren gedefinieerd en onvoldoende duidelijk waren afgebakend; dat de bepalingen inzake de stopzetting van de geheime surveillance maatregelen onvoldoende garanties boden tegen willekeurige inmenging; dat de nationale wetgeving de automatische opslag van duidelijk irrelevante gegevens toestond en onvoldoende duidelijk verschafte over de omstandigheden waarin het onderschepte materiaal zou worden opgeslagen en vernietigd; dat de vergunningsprocedures onvoldoende waren om ervoor zorg te dragen dat de geheime surveillance maatregelen alleen werden bevolen als deze "noodzakelijk in een democratische samenleving" waren; dat het toezicht op de onderscheppingen, zoals het was georganiseerd, niet voldeed aan de eisen van onafhankelijkheid en geen effectieve en continue controle mogelijk maakte; en dat de effectiviteit van de maatregelen werden ondermijnd door het ontbreken van een notificatieplicht op het punt van onderscheppingen.

Daarom stelde het Europese Hof voor de Rechten van de Mens tot slot het volgende: ‘It is significant that the shortcomings in the legal framework as identified above appear to have an impact on the actual operation of the system of secret surveillance which exists in Russia. The Court is not convinced by the Government’s assertion that all interceptions in Russia are performed lawfully on the basis of a proper judicial authorisation. The examples submitted by the applicant in the domestic proceedings and in the proceedings before the Court indicate the existence of arbitrary and abusive surveillance practices, which appear to be due to the inadequate safeguards provided by law. In view of the shortcomings identified above, the Court finds that Russian law does not meet the “quality of law” requirement and is incapable of keeping the “interference” to what is “necessary in a democratic society”. There has accordingly been a violation of Article 8 of the Convention.’[23]

Het curieuze is dat hierdoor een wat bipolaire situatie ontstaat, in ieder geval ten aanzien van artikel 8 EVRM. Enerzijds zijn er de zaken waarin klagers direct en individueel zijn getroffen in hun individuele belangen. Anderzijds beoordeelt het Hof thans ook zaken waarin *in abstracto* claims worden geaccepteerd; hierin staat de wet of het beleid als zodanig, zonder zijn gevolgen voor de maatschappij of burgers, centraal, waarbij met name naar de legitimiteit en de legaliteit van de wet wordt gekeken. Zijn de bevoegdheden van de staat en de overheidsinstanties afdoende in de wet afgebakend, zijn er voldoende waarborgen tegen machtsmisbruik, is er onafhankelijk toezicht, etc? Daarbij komt dat het EHRM in dit soort zaken bereid is om als rechter in eerste aanleg te oordelen, dus zonder dat de nationale rechtsgang helemaal is doorlopen. In feite vervult het hiermee dus de rol die constitutionele hoven in landen als Franrijk toekomt. De vraag is hoe dit zich precies verhoudt tot het idee van mensenrechtenbescherming; als een zaak niet gaat over de impact van een wet of beleid op de mensenrechten, is het dan nog geëigend voor een mensenrechtenhof om zich daarover uit te spreken?

3. Activistische rol van het HvJ: *Digital Rights Ireland* en *Google Spain*

Interessant is dat de Europese Unie zich steeds meer wil profileren op het terrein van privacy en gegevensbescherming. Aanvankelijk was er een redelijk heldere verdeling in taken tussen de Raad van Europe en de Europese Unie. De Raad van Europa richtte zich met name op de mensenrechten en de Europese Unie met name op het sociaaleconomische beleid. De

[23] Zakaraov, paragraaf 302.

Raad van Europa beschermt het recht op privacy onder meer in het EVRM en het recht op gegevensbescherming eerst in een aantal resoluties uit de jaren ’70 en thans middels de Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data uit 1981. Langzamerhand profileert de EU zich echter steeds meer op dit terrein. In 1995 kwam het met de Richtlijn bescherming persoonsgegevens. Deze was sterk geënt op de Conventie uit 1981, maar had een andere basis, namelijk niet de bescherming van de privacy, maar de regulering van de vrije markt in persoonsgegevens (gezien het feit dat de EU toen nog voornamelijk competenties had in deze sfeer, waarover meer in sectie 6). Daarnaast heeft het een op het EVRM geënt Handvest voor de grondrechten van de Europese Unie aangenomen, met daarin onder meer het recht op privacy (artikel 7) en het recht op gegevensbescherming (artikel 8) vervat. Tot slot gedraagt het Hof van Justitie zich steeds activistischer op dit terrein, getuige de uitspraak in de Scherms zaak (zie paragraaf 4) en de zaken Digital Rights Ireland en Google Spain. Deze zullen hier kort worden toegelicht.

In Digital Rights Ireland stond centraal de Richtlijn 2006/24/EG, betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronischecommunicatiediensten of van openbare communicatienetwerken.[24] Het ging hier om wat in de volksmond is gaan heten de bewaarplicht voor telecomproviders; die moesten onder meer internetgegevens van klanten bewaren, zodat de overheid deze zou kunnen inzien in verband met misdaad- en terrorismebestrijding. Het gaat hier met name om die gegevens die nodig zijn om de bron en de bestemming van een communicatie te traceren en te identificeren, om de datum, het tijdstip en de duur van de communicatie en het type communicatie te bepalen, om de communicatieapparatuur van de gebruikers te identificeren en om de locatie van mobiele communicatieapparatuur te bepalen. Deze gegevens omvatten onder andere de naam en het adres van de abonnee, het telefoonnummer van de oproeper en het opgeroepen nummer, alsook een IP-adres voor internetdiensten. Aan de hand van deze zogenoemde meta-data kan worden nagegaan met welke persoon en via welke weg een abonnee heeft gecommuniceerd, hoe lang de communicatie heeft geduurd en vanaf welke plaats zij heeft plaatsgevonden. Daarnaast kan aan de hand van deze gegevens worden achterhaald hoe vaak de abonnee gedurende een bepaalde periode met bepaalde personen heeft gecommuniceerd. Het Hof van Justitie oordeelde onder meer dat uit deze gegevens tezamen ‘zeer precieze conclusies [kunnen] worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren.’[25] Onder meer omdat het hier gaat om het vrij onbeperkt en ongerichte verzamelen van gegevens, ook over burgers jegens wie geen concrete verdenking bestaat, oordeelde het Hof dat Richtlijn 2006/24/EG in strijd was met het Handvest en derhalve ongeldig was.

De zaak *Google Spain* is beter bekend komen te staan als de *Right to be Forgotten*-zaak, waarin het zogenoemde recht om vergeten te worden werd aangenomen door het Hof van Justitie. Opmerkelijk is dat dit recht niet expliciet wordt genoemd in de thans geldende Richtlijn bescherming persoonsgegevens, maar wel in de aanstondse Algemene Verordening Gegevensbescherming, die op termijn de Richtlijn zal vervangen. Toch heeft het Hof op basis van de Richtlijn en het daarin vervatte recht om gegevens te laten verwijderen een dergelijk recht geconstrueerd. Artikel 12 van de Richtlijn, betreffende het recht van toegang, stelt:

[24] Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronischecommunicatiediensten of van openbare communicatienetwerken en tot wijziging van richtlijn 2002/58/EG, is ongeldig.

[25] Digital Rights Ireland, paragraaf 27.

> ‘De Lid-Staten waarborgen elke betrokkene het recht van de voor de verwerking verantwoordelijke te verkrijgen: (…) b) naar gelang van het geval, de rectificatie, de uitwissing of de afscherming van de gegevens waarvan de verwerking niet overeenstemt met de bepalingen van deze richtlijn, met name op grond van het onvolledige of onjuiste karakter van de gegevens; c) kennisgeving van derden aan wie de gegevens zijn verstrekt, van elke rectificatie, uitwissing of afscherming, uitgevoerd overeenkomstig punt b), tenzij zulks onmogelijk blijkt of onevenredig veel moeite kost.’

Artikel 14 van de Richtlijn, ten aanzien van het recht van verzet, bepaalt onder meer:

> ‘De Lid-Staten kennen de betrokkene het recht toe: a) zich ten minste in de gevallen, bedoeld in artikel 7, onder e) en f), te allen tijde om zwaarwegende en gerechtvaardigde redenen die verband houden met zijn bijzondere situatie ertegen te verzetten dat hem betreffende gegevens het voorwerp van een verwerking vormen, behoudens andersluidende bepalingen in de nationale wetgeving. In geval van gerechtvaardigd verzet mag de door de voor de verwerking verantwoordelijke persoon verrichte verwerking niet langer op deze gegevens betrekking hebben’.

In de zaak *Google Spain* ging het om een man die ooit in de financiële problemen was geraakt. Dit had in de lokale krant gestaan, de lokale krant had vervolgens jaren later het archief gedigitaliseerd en Google had dit archief op zijn beurt weer geïndexeerd, met als gevolg dat als men nu op de naam van deze man zocht in de zoekmachine, dit bericht gelijk zichtbaar werd, terwijl het betreffende feit al vele jaren geleden had plaatsgevonden. Het HvJ oordeelde ten aanzien hiervan onder meer dat de

> ‘artikelen 12, sub b, en 14, eerste alinea, sub a, van richtlijn 95/46 moeten aldus worden uitgelegd dat, ter naleving van de in deze bepalingen voorziene rechten en voor zover aan de in deze bepalingen gestelde voorwaarden daadwerkelijk is voldaan, de exploitant van een zoekmachine verplicht is om van de resultatenlijst die na een zoekopdracht op de naam van een persoon wordt weergegeven, de koppelingen te verwijderen naar door derden gepubliceerde webpagina’s waarop informatie over deze persoon is te vinden, ook indien deze naam of deze informatie niet vooraf of gelijktijdig van deze webpagina’s is gewist en, in voorkomend geval, zelfs wanneer de publicatie ervan op deze webpagina’s op zich rechtmatig is.’[26]

Over het effect van deze zaken op de nationale rechtspraktijk is veel gezegd en geschreven. Dat valt helaas buiten de reikwijdte van dit stuk. Eerder verscheen in dit blad bijvoorbeeld de zeer inzichtelijke analyse van Stefan Kulk en Frederik Zuiderveen Borgesius over de invloed van de *Google Spain* zaak op de Nederlandse rechtspraktijk.[27] Zij hebben daarnaast nog een aantal andere artikelen op dit punt geschreven.[28] Ten aanzien van de praktische implicaties van de uitspraak van de *Digital Rights Ireland* zaak kan de lezer onder meer te rade gaan bij het werk van Hielke Hijmans[29] en Kristian Irion.[30]

---

[26] Google Spain, conclusies.
[27] S. Kulk & F. Zuiderveen Borgesius, ‘De implicaties van het Google Spain-Arrest voor de vrijheid van meningsuiting’, NTM|NJCM-Bull. jrg. 40, 2015, nr. 1.
[28] S Kulk & F.J. Zuiderveen Borgesius, ‘Google Spain v. González: Did the Court Forget About Freedom of Expression?’, European Journal of Risk Regulation 2014, afl. 3, p. 389-398. S. Kulk, dr. F.J. Zuiderveen Borgesius, ‘Freedom of Expression and 'Right to Be Forgotten' Cases in the Netherlands after Google Spain’, European Data Protection Law Review, 2015-2, p. 113-125.
[29] H. Hijmans, ‘De ongeldigverklaring van de Dataretentierichtlijn: een nieuwe stap in de bescherming van de grondrechten door het Hof van Justitie’, Nederlands tijdschrift voor Europees recht, 2014-7.

4. Stop op transnationale gegevensstromen: *Schrems* en de *Safe Harbor Agreement*

Het verloop van de zaak *Schrems* 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 Dataprotectie 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 verschaft. Bovendien stelde zij 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 Richtlijn bescherming persoonsgegevens bepaalt in artikel 25:

> 'De Lid-Staten bepalen dat persoonsgegevens die aan een verwerking worden onderworpen of die bestemd zijn om na doorgifte te worden verwerkt, slechts naar een derde land mogen worden doorgegeven indien, onverminderd de naleving van de nationale bepalingen die zijn vastgesteld ter uitvoering van de andere bepalingen van deze richtlijn, dat land een passend beschermingsniveau waarborgt.'

Het artikel kent vervolgens echter de Commissie de bevoegdheid toe om ten aanzien van een bepaald land te bepalen dat het wel of geen passende waarborgen kent ten aanzien van de bescherming van persoonsgegevens. De Commissie had dit inderdaad gedaan in een beschikking, namelijk Beschikking 2000/520,[31] waarnaar de Commissioner verwijst. Het 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 Unie[32] 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

---

[30] M.-P. Granger & dr. K. Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland', European Law Review, 2014-6, p. 835-850.

[31] 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 (Kennisgeving geschied onder nummer C(2000) 2441).

[32] https://www.ecb.europa.eu/ecb/legal/pdf/c_32620121026nl.pdf

het HvJ ongeldig is verklaard, mogen de lidstaten en hun organen, waaronder de onafhankelijke toezichthoudende 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.

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.'

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.'[33]

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

[33] HvJ, Schrems, r.o. 105.

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. 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. De melding zweeft al een tijd boven de markt dat de EU en de VS een akkoord zouden hebben bereikt over een nieuwe, aangepaste 'safe harbor agreement'.[34] 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.'[35] Het onderwerp van transnationale dataverwerking en gegevensdoorvoer zal derhalve voorlopig nog wel op de politieke agenda blijven staan.

5. Hocus pocus pilatus uitspraak: *Coty t. Stadtsparkasse* en *Delfi t. Estland*

Terwijl mensenrechten aanvankelijk primair zagen op de bescherming van fundamentele belangen en kernwaardes, gaat het thans steeds vaker om de bescherming van vrij particuliere belangen. Waar mensenrechten aanvankelijk vooral zagen op het inperken van overheidsmacht, gaat het thans steeds vaker om de botsing van twee individuele belangen, die beide worden verheven tot mensenrechten. Terwijl er aanvankelijk voornamelijk een principiële toetst werd toegepast door mensenrechtenhoven, zoals betreffende de vraag of een inperking is voorgeschreven bij wet, noodzakelijk is in een democratische samenleving en überhaupt een legitiem doel dient, gaat het tegenwoordig steeds meer om het afwegen van de verschillende, al dan niet particuliere, belangen. Terwijl aanvankelijk vooral werd ingezet op de bredere impact van uitspraken, stellen hoven thans vaak dat zij uitsluitend uitspraak doen op een *case by case* basis, waarbij, rekening houdend met de omstandigheden van het geval, slechts over die ene, particuliere zaak uitspraak wordt gedaan. Deze ontwikkeling is uiteraard niet nieuw, maar lijkt wel steeds prominenter in de jurisprudentie ten aanzien van het recht op privacy en het recht op gegevensbescherming van zowel het Europees Hof voor de Rechten van de Mens als het Europees Hof van Justitie. De zaken *Coty t. Stadtsparkasse* en *Delfi t. Estland* zijn hiervoor illustratief.

De zaak Coty betreft een relatief eenvoudig zaak. Een merkhouder vermoedt dat iemand illegaal zijn merk verkoopt via een site en doet zich voor als koper; vervolgens vraagt het de site om de identiteit van de verkoper en die krijgt het. Deze persoon B. stelt echter, alhoewel de houder te zijn van het account waarmee het product is verkocht, niet zelf de transactie te hebben verricht. Coty gaat naar de bank (Stadtsparkasse) waarop het bedrag is gestort; die weigert echter de identiteit van de rekeninghouder vrij te geven, met een beroep op het bankgeheim. Een Duitse rechter stelt Coty in het gelijk, maar in hoger beroep wordt de

[34] http://europa.eu/rapid/pressrelease_IP-16-216_en.htm.
[35] www.rtlnieuws.nl/economie/home/eu-en-vs-sluitenpolitieke-deal-om-je-data-tebeschermen.

bank in het gelijk gesteld – er komt een prejudiciële vraag aan het HvJ. Als het Hof deze zaak op een inhoudelijke wijze had willen behandelen, waarbij zijn uitspraak een grotere, maatschappelijke waarde zou hebben gehad, zou de volgende vragen hebben kunnen nalopen. (1) Kan Stadtparkasse in deze zaak een beroep doen op het bankgeheim en daaraan verbonden, welke waarde vertegenwoordigt het bankgeheim eigenlijk? Het wordt immers vaak gezegd dat geheimhouding in deze een *conditio sine qua non* is voor het bankwezen. Net zoals de vertrouwelijkheid tussen advocaat en cliënt een voorwaarde is voor een goede verdediging en de gezondheidszorg in sterk verminderde mate kan functioneren als de vertrouwelijkheid tussen arts en patiënt niet is gewaarborgd, is voor veel mensen ook de vertrouwelijkheid van hun financiële gegevens een voorwaarde om hun geld op een bank te zetten. (2) Is er een inbreuk op dit bankgeheim door het vrijgeven van de identiteit van een cliënt of is het bankgeheim vooral gericht op de financiële situatie van een spaarder? (3) Is deze inbreuk voorgeschreven bij wet? Dit is twijfelachtig omdat Coty een beroep doet op een bepaling uit het Europese recht waarin is vervat dat een dergelijke beperking kan worden opgelegd aan diensten die op commerciele schaal worden gebruikt voor het schenden van het intellectueel eigendom. Het is zeer de vraag of daar in casu sprake van is, alleen al omdat het onzeker is of de dienst van de bank is 'gebruikt' voor de inbreuk als zodanig, of dat het daarbij veeleer gaat om bijvoorbeeld het platform waarop het product is verkocht. (4) Dient de inbreuk op het bankgeheim een legitiem doel, bijvoorbeeld de bescherming van de (merk)rechten van anderen? Daarvan lijkt in casu inderdaad sprake. (5) Is de inbreuk noodzakelijk in een democratische samenleving? Dat is zeer de vraag, niet alleen omdat een beperking op het bankgeheim, gezien het maatschappelijke belang dat hiermee is gemoeid, slechts in uitzonderlijke gevallen geoorloofd zal zijn, en het zeer de vraag is of het commerciële belang van een parfumhouder in kwestie ten aanzien van één illegale verkoop zo'n zwaarwegend belang is, maar ook omdat Coty reeds de identiteit van B. kende en op basis daarvan naar de rechter had kunnen stappen; het was dan aan B. geweest te bewijzen dat hij, alhoewel de houder van het account in kwestie, niet de daadwerkelijke verkoop heeft verricht.

Het Hof van Justitie kiest echter een ander pad. Ten eerste, en wellicht het belangrijkste, het herformuleert de zaak van Coty tegen Stadtsparkasse tot een zaak tussen Coty en B. – het brengt dus een persoon in het spel, die geen partij was in de zaak. Ten tweede stelt het dat het hier niet gaat om de vraag of een maatschappelijk principe, namelijk het bankgeheim, in casu in het geding was, in hoeverre en onder welke omstandigheden hierop een uitzondering kan worden gemaakt en of de onderhavige zaak aan deze omstandigheden voldoet, maar om een botsing van twee particuliere belangen, namelijk het belang van Coty ten aanzien van het beschermen van zijn parfummerk en van B. ten aanzien van de bescherming van zijn persoonsgegevens, namelijk om zijn identiteit te beschermen. Ten derde verheft het deze twee vrij banale belangen tot fundamentele rechten, namelijk tot een botsing tussen artikel 17 lid 2 en artikel 8 van het Handvest. Ten vierde gaat het niet in op de meer fundamentele vragen rondom de wettelijke basis van de inbreuk en de noodzakelijkheid daarvan, gezien het feit dat Coty reeds de identiteit van B. had vastgesteld, maar gaat het volgens het Hof in deze zaak om een afweging van verschillende belangen – het zogenoemde 'balancing'. Ten vijfde en tot slot weegt het deze belangen af op een volstrekt onheldere wijze (het geeft niet aan hoe deze belangen worden gewogen, welke schaal daarbij wordt gehanteerd, welke gewichten het aan welke aspecten *worden* toegekend, etc.) en komt het een particulier oordeel, dat uitblinkt in nietszeggendheid, namelijk dat een bankgeheim nooit absoluut kan zijn en dat in zoverre de Duitse wet als zodanig moet worden begrepen (iets dat niet is onderzocht of besproken in deze zaak), deze in strijd moet worden geacht met het Europese recht.

De zaak *Delfi t. Estland* volgt eenzelfde pad. Het betreft hier een internetplatform ala nu.nl. Er verschijnt een nieuwsbericht op de site geplaatst door Delfi over een bedrijf, waarvan L. enig aandeelhouder is, dat van plan is een veerdienst te beginnen en dat daartoe een aantal wegen over het ijs zal vernietigen. Het bericht zelf is genuanceerd en objectief; onder het bericht verschijnen echter een aantal gebruikersreacties die minder genuanceerd zijn. L. vraagt Delfi een klein aantal daarvan, namelijk 20, te verwijderen en om een schadevergoeding; Delfi verwijdert de berichten, maar weigert een schadevergoeding te betalen, waarop L. naar de rechter stapt. Uiteindelijk komt de zaak voor het EHRM, namelijk onder artikel 10 EVRM. Het EHRM had de zaak als volgt kunnen behandelen. (1) Komt Delfi eigenlijk wel een beroep toe op de vrijheid van meningsuiting? Het betreft hier een site waarbij gebruikers reacties kunnen plaatsen, waarop Delfi zelf geen invloed heeft. Bovendien ontkent Delfi zelf de auteur of redacteur van de gebruikersreacties te zijn. Delfi stelt dan ook expliciet dat het niet onder de vrijheid van meningsuiting valt, maar onder de e-Commerce Richtlijn, die ziet op de aansprakelijkheid van internet providers. (2) Is er sprake van een inbreuk van dit recht? De vraag is onder meer of het betalen van een boete voor een smadelijke opmerking als gemaakt door een gebruiker aan het adres van L. kan worden gezien als een inbreuk of inperking van dit recht. (3) Was de inbreuk voorgeschreven bij wet in die zin dat de beperking redelijkerwijs was te voorzien voor Delfi? Dit is zeer de vraag omdat er hier twee verschillende regimes spelen, die van de e-Commerce Richtlijn van de Europese Unie en die van de vrijheid van meningsuiting, als vervat in het EVRM van de Raad van Europa. Het eerste geeft passieve internet intermediairs als Delfi uitsluiting van aansprakelijkheid, als zij meewerken aan het zogenoemde notice-and-takedown systeem (een persoon als L. stuurt bijvoorbeeld een notificatie over een inbreuk en Defli is daarop gehouden het materiaal te verwijderen, de take down), waar Delfi zich in casu inderdaad aan heeft gehouden. Het tweede kent personen en bedrijven die zich op de vrijheid van meningsuiting beroepen een relatief grote vrijheid toe, die evenwel met tal van plichten komt. Het is vaak voor internet intermediairs volstrekt onduidelijk onder welk regime zij vallen; dit wordt bevestigd door de nationale rechtsgang waar Delfi soms onder het ene en soms onder het andere regime wordt beoordeeld, wat soms tot een vrijspraak en soms tot een Verordening leidt. (4) Dient de inbreking een legitiem belang? Dat lijkt hier het geval, omdat het gaat om de bescherming van de rechten van derden, namelijk die van L. en zijn bedrijf. (5) Is de inperking noodzakelijk in een democratische samenleving? Dit is sterk de vraag. Het gaat hier om een zeer grote internetsite, waarop dagelijks vele gebruikersreacties verschijnen. Ook onder dit nieuwsbericht verschenen er tal van reacties. Daarvan werden er 20 door L. als onrechtmatig aangemerkt en zelfs van deze 20 was de meerderheid eerder kinderachtig dan smadelijk, zoals ‘ik pis in je oor en poep op je hoofd’ en ‘deugniet!’.

Het EHRM bewandelt echter een andere weg. Ten eerste kiest het er wederom voor om de zaak te herformuleren, van een zaak tussen Delfi en Estland, tot een zaak tussen Delfi en L.; net zoals het Hof van Justitie brengt het dus een persoon in het spel die geen partij is bij de rechtszaak. Ten tweede stelt het dat het hier niet gaat om de vraag of de vrijheid van meningsuiting in het geding was, in hoeverre en onder welke omstandigheden hier een inbreuk op kan worden gemaakt en of daar in het onderhavige geval sprake van was, maar om een botsing van de belangen van de twee partijen. Ten derde kiest het ervoor om deze vrij banale belangen te verheffen tot mensenrechten. Het belang van Delfi om geen boete te hoeven te betalen is een schending van het recht op vrijheid van meningsuiting en het belang van L. wordt beschermd onder het recht op reputatie als beschermd door artikel 8 EVRM, het recht op privacy. Met name deze laatste keuze is opmerkelijk, omdat de opstellers van het EVRM er expliciet voor hebben gekozen om het recht op bescherming van reputatie en eer en goede naam geen subjectief recht te maken onder artikel 8 EVRM (in tegenstelling tot artikel 12 UVRM), maar als één van de gronden te zien op basis waarvan een staat een legitieme

uitzondering op het recht van meningsuiting kan maken (het is vervat in lid 2 van artikel 10 EVRM). Hiermee is het dus een algemeen belang dat een grond kan zijn voor de staat om een individueel recht te beperken en niet het particuliere belang van een specifiek individu dat geen deugniet wil worden genoemd. Ten vierde gaat het Hof nauwelijks in op de vraag of de inperking is voorgeschreven bij wet en of de inbreuk noodzakelijk is in een democratische samenleving, maar kiest het er in plaats daarvan voor om de verschillende particuliere belangen tegen elkaar af te wegen. Ten vijfde en tot slot is het wederom volstrekt onduidelijk hoe het de diverse belangen eigenlijk afweegt, hoe het gewichten toekent, op welke schaal het weegt, etc. Het EHRM tovert een aantal criteria uit de hogehoed, waarbij het echter onduidelijk blijft hoe het komt tot de keuze voor deze criteria. De zaken Coty en Delfi zijn twee recente voorbeelden van hoe het mensenrechtenkader langzaam wordt uitgekleed, maar zij staan symbool voor een veel bredere en meeromvattende tendens.

6. Nieuwe regels die toch erg oud zijn: de Algemene Verordening Persoonsgegevens

Er is een interessante dynamiek gaande tussen het recht op privacy en het recht op gegevensbescherming. Het recht op gegevensbescherming is van recentere aard en vindt zijn oorsprong in de Amerikaanse Fair Information Practices, de eerder genoemde resoluties van de Raad van Europa en een de regels in een aantal Europese landen, zoals Duitsland, Zweden en Oostenrijk op dit punt, die allemaal begin jaren ’70 werden ontwikkeld. Dit recht is dan ook als zodanig niet opgenomen in het EVRM, dat uit 1950 stamt; wel wordt het door het EHRM beschermd, voornamelijk onder het recht op privacy, artikel 8 EVRM. Ook in de resoluties en de Conventie uit 1981 wordt een expliciete koppeling met het recht op privéleven gemaakt. Interessant is dat het begrip ‘persoonsgegeven’ veel wijder is dan het ‘privéleven’ of dan gevoelige gegevens die de privacy van burgers raken; het gaat bij een persoonsgegeven om ieder gegeven dat een persoon mogelijkerwijs kan identificeren, ook volstrekt publieke en ongevoelige gegevens, zoals ‘die man daar, naast de lantaarnpaal, met het gele shirt’. Om te voorkomen dat alle zaken omtrent de verwerking van persoonsgegevens onder artikel 8 EVRM zouden komen te vallen, stelde het EHRM aanvankelijk dat de verwerking van persoonsgegevens slechts onder de reikwijdte van het recht op privacy viel als het individu in zijn privacy en/of privéleven was geschaad. Langzamerhand is deze lat echter verdwenen en worden steeds meer zaken onder het recht op privacy besproken, zelfs als het gaat om het verzamelen van bijvoorbeeld metadata. De twee rechten raken derhalve steeds meer met elkaar vervlochten. In de Europese Unie valt echter een tegengestelde tendens te bespeuren. Niet alleen worden de twee rechten expliciet in een andere bepaling in het Handvest beschermd, ook de Verordening maakt hierin een expliciete keuze. De Richtlijn bescherming persoonsgegevens maakt nog een expliciete link met de bescherming van de persoonlijke levenssfeer, bijvoorbeeld in artikel 1, betreffende de werkingssfeer van de Richtlijn, ‘De Lid-Staten waarborgen in verband met de verwerking van persoonsgegevens, overeenkomstig de bepalingen van deze richtlijn, de bescherming van de fundamentele rechten en vrijheden van natuurlijke personen, inzonderheid van het recht op persoonlijke levenssfeer’, en maakt ook verder in de tekst op tal van punten een expliciete koppeling met het recht op privacy. De Algemene Verordening Gegevensbescherming, daarentegen, ontkoppelt deze twee rechten in zijn geheel. Artikel 1 stelt ‘This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.’ Daarnaast wordt er geen enkele keer verwezen naar het recht op privacy of de bescherming van de persoonlijke levenssfeer. Zelfs bekende termen als ‘Privacy by design’ en ‘Privacy impact assessments’ zijn vervangen door ‘Data protection by design’ en ‘Data protection impact assessments’.

Daarnaast is het interessant dat er binnen de EU een soort juridisch fundamentalisme aan het ontstaan is. Rechten en belangen worden op een steeds hoger niveau beschermd. Het recht op gegevensbescherming wordt bijvoorbeeld een fundamenteel recht genoemd, wat zeer dubieus is omdat zelfs het publiceren van een onschuldig vakantiekiekje op Facebook al een verwerking van persoonsgegevens kan zijn. Alhoewel ook onder het EVRM het begrip mensenrecht vrijwel grenzeloos lijkt te zijn, is dit voor vele commentatoren een stap te ver. Ook is de juridische grondslag voor de Regulering, in tegenstelling tot de Richtlijn, niet langer het reguleren van de vrije markt, maar de bescherming van persoonsgegevens Artikel 16 van het Verdrag Betreffende de Werking van de Europese Unie stelt:

> '1. Eenieder heeft recht op bescherming van zijn persoonsgegevens. 2. Het Europees Parlement en de Raad stellen volgens de gewone wetgevingsprocedure de voorschriften vast betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie, alsook door de lidstaten, bij de uitoefening van activiteiten die binnen het toepassingsgebied van het recht van de Unie vallen, alsmede de voorschriften betreffende het vrij verkeer van die gegevens. Op de naleving van deze voorschriften wordt toezicht uitgeoefend door onafhankelijke autoriteiten. (…)De op basis van dit artikel vastgestelde voorschriften doen geen afbreuk aan de in artikel 39 van het Verdrag betreffende de Europese Unie bedoelde specifieke voorschriften.'

In tegenstelling tot een Richtlijn hoeven de regels uit een Verordening niet te worden geïmplementeerd in de diverse nationale rechtsordes, aangezien zij directe werking hebben. Wat betreft de inhoud is de Algemene Verordening Gegevensbescherming tamelijk behoudend. De regels uit de Richtlijn dateren uit het begin van het internettijdperk en van voor het tijdperk van de Internet of Things, Big Data, smart applications en cloud computing. Toch blijven de materiele regels in grote lijnen behouden. Het dataminimalisatieprincipe blijft overeind, het doelbindingsprincipe, het vereiste van datakwaliteit, van specifieke en legitieme doeleinden en van transparantie evenzo. De datasubjecten krijgen iets ruimere rechten, zoals het recht om vergeten te worden en het recht op dataportabiliteit (waarbij een gebruiker bijvoorbeeld het recht heeft om zijn Facebook profiel mee te nemen naar een ander sociaal netwerk), maar in feite zijn deze regels zo beperkt en kennen ze zoveel mitsen en maren dat deze bepalingen voornamelijk moeten worden geduid als een publiciteitsstunt van de Europese Commissie en in veel mindere mate als een versterking van de rechten van datasubjecten.

Het vrijwel volledig ongewijzigd laten van de materiele bepalingen uit het gegevensbeschermingsrecht wordt door velen als een gemiste kans ervaren; het zal waarschijnlijk nog weer 20 jaar duren alvorens er een herziening zal komen van de Algemene Verordening Gegevensbescherming. Toch is er wel degelijk iets wezenlijks gewijzigd in de Verordening, namelijk ten aanzien van de handhaving van de materiele bepalingen. Het algemene sentiment ten aanzien van de gegevensbeschermingsregels is dat deze in wezen deugdelijk en adequaat zijn, maar dat het schort aan daadwerkelijke en effectieve handhaving daarvan. Zowel overheidsorganen, grote multinationals als ook burgers houden zich doorgaans niet aan de vigerende wet- en regelgeving. Dit heeft twee belangrijke oorzaken, naast een gebrek aan kennis over de regels en de onwil om deze te volgen. Ten eerste is het niveau van de gegevensbeschermingsregels en de handhaving daarvan met betrekking tot Europa en andere rechtsorders zeer ongelijk, waarbij uiteraard de situatie in de Verenigde Staten het meest in het oog springt. Ten tweede is het niveau van de gegevensbeschermingsregels en de handhaving daarvan tussen de EU-lidstaten onderling zeer divers. Ten aanzien van het eerste is het probleem, dat reeds aan de orde kwam bij de bespreking van de zaak Schrems, dat veel multinationals die zich bezighouden met het

verzamelen en verwerken van persoonsgegevens, zijn gevestigd in de Verenigde Staten, alwaar een over het algemeen lager beschermingsniveau ten aanzien van gegevensbescherming geldt. Daarbij komt dat ook de Amerikaanse overheid zich vaak eenvoudig toegang kan verschaffen tot de gegevens in het bezit van Amerikaanse bedrijven of Europese bedrijven die deels zijn gevestigd op het Amerikaans grondgebied. Ten tweede, door het verschil in beschermings- en handhavingsniveau binnen de EU, kunnen bedrijven effectief de regels omzeilen door zich te vestigen in landen waar de regel- en handhavingsdruk laag is, lees Ierland. Tot slot en daarnaast wordt vaak als knelpunt aangegeven dat als er eenmaal een overtreding van de regels wordt geconstateerd en als dit effectief wordt aangepakt door een handhavingsorganisatie, er doorgaans slechts waarschuwingen volgen of boetes worden opgelegd van enkele duizenden euro's, iets wat nauwelijks zoden aan de dijk zet met betrekking tot het aanpakken van multinationals als Apple, Google, Facebook, Twitter, Microsoft en Amazon.

Deze problemen worden aangepakt door de Verordening. Ten eerste heeft de Verordening directe werking, waardoor het verschil in beschermingsniveau in de EU grotendeels verdwijnt. Ten tweede wordt er ingezet op verregaande samenwerking tussen de verschillende handhavende organisaties binnen Europa, zodat bedrijven door een zogenoemde *lead Data Protection Authority*, zoals het College Bescherming Persoonsgegevens, dat thans de Autoriteit Persoonsgegevens wordt genoemd, kunnen worden aangepakt door heel Europa. Ten derde worden er tal van aanvullende plichten geïntroduceerd voor bedrijven, bijvoorbeeld om te investeren in technische maatregelen als *Data Protection by Design* en *Data Protection by Default* en in *Data Protection Impact Assessments* en om een interne *Data Protection Officer* aan te stelen, die de naleving van de regels controleert. Ook is er een uitgebreide documentatie- en auditplicht ingevoegd, ligt er meer nadruk op gedragscodes en certificaten en is er een meldplicht in het geval van datalekken. Ten vierde wordt er meer ingezet op nadere regels voor transnationale gegevensdoorvoer naar derde landen. Ten vijfde en tot slot worden er nadere regels gesteld ten aanzien van het opleggen van boetes. Zo is ten aanzien van een overtreding van een deel van de bepalingen uit de Verordening neergelegd dat er een administratieve boete van 10 miljoen euro kan worden opgelegd, of in het geval van bedrijven, tot 2% van hun wereldwijde, jaarlijkse omzet, iets wat in het geval van bijvoorbeeld Apple en Google flink kan oplopen. Voor het andere deel van de bepalingen is dit zelfs 4% van de wereldwijde jaarlijkse omzet of 20 miljoen euro boete.

7. Conclusie

Deze kroniek heeft een aantal van de belangrijkste ontwikkelingen besproken op het gebied van privacy en gegevensbescherming, voornamelijk op Europees niveau. Het heeft laten zien dat het Europees Hof voor de Rechten van de Mens zich enerzijds steeds meer richt op het beschermen van particuliere belangen, waarbij zich de vraag opdringt of het daarbij daadwerkelijk nog om mensenrechten gaat, en anderzijds er nu voor heeft gekozen om wetten op het rechtmatigheid en legitimiteit te beoordelen, zelfs als er geen directe schade aan de mensenrechten van particulieren is gedaan. De kroniek heeft ook laten zien dat het Europees Hof van Justitie prominenter op de voorgrond is getreden en zich activistischer opstelt. Het deinst er niet voor terug om richtlijnen van de Europese Unie en Beschikkingen van de Europese Commissie ongeldig te verklaren, noch om nieuwe rechten, zoals het recht om vergeten te worden, in de huidige Richtlijn bescherming persoonsgegevens te lezen. Hierdoor komt onder meer de vrije doorvoer van persoonsgegevens tussen de Verenigde Staten en de Europese Unie onder druk te staan. De kroniek heeft belicht dat er door beide Europese hoven steeds meer wordt gekozen om verschillende al dan niet particuliere belangen tegen

elkaar af te wegen, daarbij vaak voorbij gaande aan meer rechtstatelijke waarborgen. Tot slot heeft de kroniek een snelle blik geworpen op de aanstaande Verordening Gegevensbescherming, die op termijn de huidige Richtlijn bescherming persoonsgegevens, waarop de Nederlandse Wet bescherming persoonsgegevens is gestoeld, zal vervangen. Daarin worden een aantal nieuwe rechten voor het datasubject en een aantal nieuwe verplichtingen voor de verantwoordelijke voor de gegevensverwerking geïntroduceerd. De belangrijkste wijzigingen zijn echter te vinden op het gebied van naleving en handhaving; het meest in het oog springende wat dat betreft zijn de boetes die in de toekomst kunnen worden opgelegd, die tot 20 miljoen euro of 4% van de wereldwijde jaarlijkse omzet van een bedrijf kunnen oplopen.