Maakt grenzeloos machteloos?

De veranderende rechtsmacht van de privacytoezichthouder binnen het nationale en Europese privacyrecht

mr. F.C. van der Jagt

***** Friederike van der Jagt is Senior Legal Counsel Privacy bij Avast. Zij schrijft dit preadvies op persoonlijke titel. Dit preadvies is afgerond op 24 november 2016. Zij is bijzonder grote dank verschuldigd aan mr. M.P. Vink van Rutgers & Posch advocaten, voor zijn commentaren op eerdere versies van dit preadvies.

1 Inleiding

6.30 uur, uw smartphone wekt u en in de verte hoort u het koffiezetapparaat al automatisch aangaan. In huis is het aangenaam warm, uw 'Toon' heeft zijn werk weer gedaan. Handig, al die *smart* toepassingen! U werkt wat appjes weg, checkt nog even *Facebook* en accepteert nog snel een *LinkedIn*-verzoek. Nu moet u echt uit bed, want u moet nog langs de huisarts. Misschien kunt u hem dan meteen vragen of u uw bloeddrukgegevens voortaan via uw smartphone kunt doorgeven, dat scheelt toch weer een bezoekje. Nu maar hopen dat de huisarts deze keer wel de weg in uw elektronische patiëntendossier weet te vinden, een aardige man hoor, maar wat een digibeet. Toen u de vorige keer aanbood om uw *Fitbit*-gegevens met hem te delen, keek hij u alleen maar glazig aan ... Daarna snel door naar het werk, met de trein want volgens *Flitsmeister* staan er vanochtend veel files op uw vaste route. OV-chipkaart paraat en even op de tablet een krantje lezen. Kan iemand iets doen aan die irritante *cookie*-melding die u steeds krijgt? Alleen om de melding op de site van de HEMA kunt u wel lachen; daar gebruikt men stroopwafels als *cookies* ... Ja, zelfs juristen kunnen grappig zijn! Op kantoor aangekomen snel de laptop open en via *Skype* inbellen bij die belangrijke vergadering. Een van uw collega's begint een lange monoloog, het signaal om snel de *mute*-stand aan te zetten en te kijken of u op *Instagram* en *Twitter* nog iets gemist heeft. Uw dochter wil dat u eindelijk ook iets gaat doen met *Snapchat* ... volgens haar is *Facebook* allang passé. En terwijl u vorig weekend nog *Pokemons* stond te vangen, schijnt dat ook alweer uit te zijn. U zult blij zijn als deze dag voorbij is, dan kunt u vanavond eindelijk weer eens trainen voor die halve marathon. Volgens uw *Nike+ Run Club*-app is er nog heel wat werk aan de winkel. En dan daarna welverdiend het laatste seizoen van *Narcos* op uw nieuwe smart-tv bekijken ...

Het bovenstaande zal menigeen bekend in de oren klinken. Internet, social media en de smartphone zijn onlosmakelijk met ons leven verbonden. Dit betekent eveneens dat, om gebruik te kunnen maken van alle voordelen die de technologische ontwikkelingen met zich brengen, we steeds meer informatie moeten delen. Want online is bijna niets echt gratis: u betaalt meestal met uw persoonsgegevens. Ook staan uw persoonsgegevens vaak niet meer lokaal opgeslagen, zoals vroeger bij uw huisarts in uw papieren dossier. Tegenwoordig wordt veelal gebruikgemaakt van wereldwijde *cloud*-toepassingen. U 'doet zaken' met, en bent steeds meer afhankelijk van, grote internationale spelers zoals *Google* en *Facebook*. Dit roept de vraag op, op welke wijze de Nederlandse privacytoezichthouder, de Autoriteit Persoonsgegevens (AP), ervoor kan zorgen dat uw privacy goed beschermd wordt. Of bestaat de Nederlandse rechtsmacht in het huidige tijdperk alleen nog maar op papier?

Met het begrip 'rechtsmacht van de toezichthouder' bedoel ik in dit preadvies de mogelijkheid van de nationale toezichthouder, meer in het bijzonder de AP, om haar toezichthoudende bevoegdheden, waaronder het handhavend kunnen optreden, uit te kunnen oefenen. De rechtsmacht van de AP is nauw verweven met het toepasselijke recht: de AP mag op het Nederlandse grondgebied toezicht uitoefenen op de verwerking van persoonsgegevens overeenkomstig hetgeen bij en krachtens de wet is bepaald (art. 51, eerste lid jo. art. 61 Wet bescherming persoonsgegevens jo. art. 5:11 Algemene wet bestuursrecht). Om te bepalen of de AP rechtsmacht heeft, is het daarom steeds van belang om vast te stellen of de Nederlandse privacywetgeving van toepassing is. Daarom zal, na een korte uiteenzetting van het huidige privacyrechtelijke kader, aandacht worden besteed aan de problematiek omtrent de bepaling van het toepasselijke nationale recht. Hieruit zal blijken dat de AP ook rechtsmacht kan hebben over gegevensverwerkingen die feitelijk *buiten* het Nederlandse grondgebied plaatsvinden. Daarna zal worden

gekeken welke vraagstukken het bepalen van de rechtsmacht in de praktijk oproept. Want hoe ver kan de territoriale reikwijdte van de Privacyrichtlijn, en daarmee de rechtsmacht van de nationale toezichthouders, worden opgerekt? En welke mogelijkheden heeft een nationale toezichthouder om op te treden tegen privacyschendingen op zijn grondgebied, als zijn nationale recht niet van toepassing is?

Tot slot wordt bezien of de nieuwe Europese Privacyverordening gevolgen heeft voor de rechtsmacht van de verschillende nationale privacytoezichthouders en worden twee stellingen geponeerd.

2 Een korte schets van het huidige privacyrechtelijke kader

2.1 Internationaalrechtelijk kader

Het recht op privéleven, ofwel het recht op privacy, is een klassiek vrijheidsrecht dat uitgaat van de bescherming van het individu op inbreuken van buitenaf op zijn privéleven.[1] Het omvat de bescherming van het gezinsleven (*relationele privacy*), de bescherming van iemands woning (*ruimtelijke privacy*) en de bescherming van persoonsgegevens (*informationele privacy*). Dit preadvies richt zich op de rechtsmacht van de nationale toezichthouders in het kader van de informationele privacy.

Het fundamentele recht op privacy is internationaal verankerd in artikel 12 van de Universele Verklaring van de Rechten van de Mens en artikel 17 van het Internationale Verdrag inzake Burgerrechten en Politieke Rechten.

Daarnaast is het recht op informationele privacy uitgewerkt in het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens uit 1981 (ook wel het Verdrag van Straatsburg of Conventie 108 genoemd, hierna: 'Verdrag van Straatsburg'), dat door Nederland in 1993 is geratificeerd.[2] Het aanvullende protocol[3] bij dit verdrag verplicht verdragspartijen een onafhankelijke toezichthoudende autoriteit in te stellen. In Nederland is dit de AP.

2.2 Europeesrechtelijk kader

2.2.1 Richtlijnen en verordeningen

Het recht op informationele privacy is in diverse wetgevende instrumenten neergelegd. De Europese Privacyrichtlijn[4] van 1995 vormt het belangrijkste startpunt. De Privacyrichtlijn is een interne marktrichtlijn en beoogt dan ook om het vrije verkeer van persoonsgegevens binnen de Europese Unie te waarborgen.[5] Daarnaast heeft de Privacyrichtlijn ten doel het fundamentele recht op informationele privacy te beschermen en te versterken, onder meer door de verduidelijking van het Verdrag van Straatsburg.[6] Door de snelle technologische ontwikkelingen (de Privacyrichtlijn dateert van voor de opkomst van het internet

[1] Par. 2 is gebaseerd op een eerdere bijdrage van de auteur in J.H. Gerards e.a., *Grondrechten. De nationale, Europese en internationale dimensie*, Nijmegen: Ars Aequi Libri 2013, p. 163-183.

[2] Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, Raad van Europa, 28 januari 1981, *Trb*. 1988, 7.

[3] Aanvullend Protocol bij het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens inzake toezichthoudende autoriteiten en grensoverschrijdend verkeer van gegevens, Straatsburg 8 november 2001, *Trb*. 2003, 122.

[4] 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 (*PbEG* 1995, L 281/31).

[5] Zie art. 1 Privacyrichtlijn.

[6] Zie overweging 3, 10 en 11 Privacyrichtlijn. Hierbij zij opgemerkt dat de Privacyrichtlijn een ruimer toepassingsbereik kent dan het Verdrag van Straatsburg, omdat onder bepaalde omstandigheden ook de niet-geautomatiseerde verwerking van persoonsgegevens binnen de reikwijdte van de Privacyrichtlijn valt.

en social media) sloot de Privacyrichtlijn niet langer aan op onze huidige *data-driven* samenleving. Na een lange wetgevingsprocedure is dit voorjaar de Europese Privacyverordening[7] aangenomen, die de Privacyrichtlijn zal gaan vervangen. De Privacyverordening zal vanaf 25 mei 2018 rechtstreeks van toepassing zijn: in tegenstelling tot een richtlijn hoeven de rechten en verplichtingen van een verordening niet te worden omgezet in nationale wetgeving, maar gelden zij rechtstreeks. In het vervolg van dit preadvies zal nader worden ingegaan op de gevolgen die de nieuwe Privacyverordening heeft voor de rechtsmacht van nationale privacytoezichthouders, en in het bijzonder de AP, binnen het privacyrecht.

Naast de algemene Privacyrichtlijn geldt een specifieke en aanvullende richtlijn voor het verwerken van persoonsgegevens met betrekking tot elektronische communicatie, de ePrivacyrichtlijn.[8] De ePrivacyrichtlijn bevat regels over onder meer het gebruik van *cookies* en het verzenden van spam. In Nederland is de ePrivacyrichtlijn geïmplementeerd in de Telecommunicatiewet. Onlangs heeft de Europese Commissie een publieke consultatie voor de herziening van de ePrivacyrichtlijn afgerond en het herzieningsvoorstel wordt begin 2017 verwacht.[9]

Volledigheidshalve zij opgemerkt dat de Europese instellingen, organen en instanties buiten de reikwijdte van de Europese Privacyrichtlijn vallen.[10] Om te garanderen dat ook de communautaire instellingen de informationele privacy waarborgen, zijn zij onderworpen aan Verordening 45/2001.[11]

Gelet op de reikwijdte van dit preadvies zullen de ePrivacyrichtlijn en de nationale uitwerking daarvan in de Telecommunicatiewet, alsmede Verordening 45/2001, buiten beschouwing worden gelaten.[12]

---

[7] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EC (algemene verordening gegevensbescherming), (*PbEU* 2016, L 119/1).

[8] Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (*PbEG* 2002, L 201/37), aangepast door Richtlijn 2009/136 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming (*PbEU* 2009, L 337/11).

[9] Zie voor de laatste stand van zaken: https://ec.europa.eu/digital-single-market/en/online-privacy.

[10] Zie art. 3, tweede lid, Privacyrichtlijn.

[11] Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van hun persoonsgegevens door de communautaire instellingen en organen betreffende het vrije verkeer van die gegevens (*PbEG* 2001, L 8/1).

[12] Voor de grensoverschrijdende verwerking van politiële en justitiële persoonsgegevens geldt een specifiek aanvullend Kaderbesluit (Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken, (*PbEU* 2008 L 350/60)). Dit Kaderbesluit wordt per 6 mei 2018 vervangen door de nieuwe Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016, betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (*PbEU* 2016, L 119/89). Naast het

2.2.2 Verdrag betreffende de werking van de Europese Unie en EU-Grondrechtenhandvest

Op Europees niveau is het fundamentele recht op privacy terug te vinden in artikel 8 van het Europees Verdrag van de Rechten van de Mens. In 2007 is een algemene europeesrechtelijke basis voor de bescherming van persoonsgegevens gelegd door aanpassing van artikel 16 van het Verdrag betreffende de werking van de Europese Unie.[13] Ook de verplichting tot het aanstellen van een onafhankelijke toezichthouder is hierin opgenomen. Het recht op informationele privacy is eveneens als een separaat recht – naast het algemene recht op privacy – opgenomen in artikel 8 van het EU-Grondrechtenhandvest.

2.3 Nationaalrechtelijk kader

Sinds 1983 is het recht op privacy verankerd in artikel 10 van de Grondwet. Daarin is eveneens een verplichting voor de wetgever opgenomen om de informationele privacy verder wettelijk te verankeren. Dit is nader uitgewerkt in onder meer de Wet persoonsregistraties,[14] de voorloper van de huidige Wet bescherming persoonsgegevens (Wbp).[15] De Wbp vormt de implementatie van de Europese Privacyrichtlijn. Naast de algemene Wbp zijn er diverse sectorspecifieke privacywetten, zoals de Wet basisregistratie personen en de Wet politiegegevens. Deze sectorspecifieke wetgeving wordt in dit preadvies buiten beschouwing gelaten.[16]

Kaderbesluit zijn nog diverse specifieke regelingen op het verwerken van persoonsgegevens door politie en justitie van toepassing, zoals de Schengenuitvoeringsovereenkomst.

[13] Verdrag van Lissabon tot wijziging van het Verdrag betreffende de werking van de Europese Unie en het Verdrag tot oprichting van de Europese Gemeenschap, Lissabon, 13 december 2007 (*PbEU* 2007, C 306/1).

[14] Wet van 28 december 1988, houdende regels ter bescherming van de persoonlijke levenssfeer in verband met persoonsregistraties (Wet persoonsregistraties), *Stb*. 1988, 665.

[15] Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), *Stb.* 2000, 302.

[16] Volledigheidshalve zij opgemerkt dat op de BES-eilanden een aangepaste Wbp geldt, de Wbp BES, welke in dit preadvies buiten beschouwing wordt gelaten.

3 Toepasselijk recht en toezicht

3.1 Materiële en territoriale werkingssfeer van de Privacyrichtlijn en de Wbp

3.1.1 Algemeen

Voor een goed begrip van de Europese en nationale privacyrechtelijke bepalingen is het van belang om allereerst een aantal belangrijke privacyrechtelijke begrippen nader onder de loep te nemen. Gelet op het feit dat de Wbp de Nederlandse implementatie vormt van de Europese Privacyrichtlijn, zullen beide hierna gezamenlijk worden behandeld.

Kernbegrippen in de Privacyrichtlijn en de Wbp zijn 'persoonsgegeven', 'verwerken', 'verantwoordelijke', 'betrokkene' en 'bewerker'.

Het begrip 'persoonsgegeven' dient ruim te worden uitgelegd.[17] Het gaat om elk gegeven betreffende een geïdentificeerde of identificeerbare levende natuurlijke persoon (zie art. 2, onder a, Privacyrichtlijn en art. 1, onder a, Wbp). Bij sommige gegevens ligt het voor de hand dat zij als persoonsgegeven worden aangemerkt, zoals iemands naam of mobiele telefoonnummer. Maar ook andere gegevens, zoals het MAC-adres (een uniek identificatienummer) van een mobiele telefoon of tablet, een IP-adres,[18] WiFi-gegevens en *cookies*[19] kunnen, indien zij herleidbaar zijn tot een natuurlijke persoon, worden aangemerkt als persoonsgegevens. Ook het verwerkingsbegrip wordt ruim uitgelegd: het gaat daarbij om elke handeling of elk geheel van handelingen met betrekking tot de persoonsgegevens (zie art. 2, onder b, Privacyrichtlijn en art. 1, onder b, Wbp). Hierbij kan worden gedacht aan het verzamelen, opslaan, bewaren of verspreiden van persoonsgegevens, maar ook aan het vernietigen of afschermen daarvan.
De meeste verplichtingen van de Privacyrichtlijn en de Wbp rusten op de 'verantwoordelijke': degene die alleen of tezamen met anderen het doel van en de middelen voor de gegevensverwerking vaststelt (art. 2, onder d, Privacyrichtlijn en art. 1, onder d, Wbp). De verantwoordelijke verzamelt persoonsgegevens van de 'betrokkene', ofwel degene op wie een persoonsgegeven betrekking heeft (art. 2, onder a, Privacyrichtlijn en art. 1, onder f, Wbp). De verantwoordelijke kan een derde partij inschakelen om hem te helpen bij de gegevensverwerking, bijvoorbeeld bij de opslag van persoonsgegevens – denk aan een cloudprovider zoals *Amazon* of *Microsoft*. Deze derde partij heeft geen zeggenschap over de

[17] Voor een uitgebreide analyse van het begrip 'persoonsgegeven' zie: Groep Gegevensbescherming Artikel 29, Advies 4/2007 over het begrip persoonsgegeven, *WP* 136.

[18] IP staat voor Internet Protocol. Versimpeld gezegd is een IP-adres het telefoonnummer van een computer, dat zichtbaar is voor andere computers op het internet. Recentelijk is bepaald dat ook dynamische IP-adressen, dat zijn IP-adressen die bij elke nieuwe verbinding met het internet wijzigen, onder bepaalde omstandigheden als persoonsgegeven kunnen worden aangemerkt, zie HvJEU 19 oktober 2016, C-582/14, ECLI:EU:C:2016:779 (*Breyer*).

[19] WiFi-gegevens zijn gegevens over en afkomstig uit draadloze netwerken. *Cookies* zijn kleine tekstbestandjes die door een webserver naar een browser worden gestuurd die toegang tot die server zoekt. De browser bewaart deze bestandjes en communiceert ze automatisch aan de oorspronkelijke webserver wanneer de browser toegang zoekt tot de webserver. Met behulp van *tracking cookies* kan het surfgedrag van een gebruiker worden gevolgd en is het mogelijk om aan gebruikers gepersonaliseerde advertenties te tonen. Art. 11.7a, vierde lid, van de Telecommunicatiewet (Tw) creëert een rechtsvermoeden voor het verwerken van persoonsgegevens bij het gebruik van *tracking cookies* en bepaalde analytische *cookies* in de zin van art. 11.7a, eerste lid, Tw.

persoonsgegevens: hij handelt in opdracht van de verantwoordelijke en mag de persoonsgegevens niet voor eigen doeleinden gebruiken. Een dergelijke partij wordt aangemerkt als 'verwerker' of 'bewerker' (art. 2, onder e, Privacyrichtlijn en art. 1, onder e, Wbp).

3.1.2 Materiële werkingssfeer

De Privacyrichtlijn en de Wbp zijn van toepassing wanneer er sprake is van de *geheel of gedeeltelijk geautomatiseerde verwerking* van persoonsgegevens. Ook de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of bedoeld zijn om in een bestand te worden opgenomen, valt binnen de reikwijdte van de Privacyrichtlijn en de Wbp (zie art. 3, eerste lid, Privacyrichtlijn en art. 2, eerste lid, Wbp). Bij een bestand moet het gaan om een gestructureerd geheel van persoonsgegevens dat betrekking heeft op meerdere personen en dat volgens bepaalde criteria toegankelijk is (zie art. 2, onder c, Privacyrichtlijn en art. 1, onder c, Wbp). Gedacht kan worden aan een geordende papieren administratie van patiëntendossiers.[20]

De materiële werkingssfeer van Privacyrichtlijn wordt verder beperkt door de toepassingssfeer van het Gemeenschapsrecht: activiteiten met betrekking tot openbare veiligheid, defensie en staatsveiligheid, alsmede activiteiten op het gebied van het strafrecht vallen niet onder de toepassingssfeer van het Gemeenschapsrecht en derhalve ook niet onder de Privacyrichtlijn (zie overweging 13 en art. 3, tweede lid, Privacyrichtlijn). Dit is in de Wbp vertaald in artikel 2, tweede lid, onder b t/m f, Wbp: de Wbp is niet van toepassing op de verwerking van persoonsgegevens (1) door de inlichtingen- en veiligheidsdiensten, (2) door de politie, voor zover het gaat om de uitvoering van de politietaak, (3) bij of krachtens de Wet gemeentelijke basisadministratie persoonsgegevens, (4) ten behoeve van de uitvoering van de Wet justitiële en strafvorderlijke gegevens, en (5) ten behoeve van de uitvoering van de Kieswet.
Daarnaast valt de verwerking van persoonsgegevens door een natuurlijke persoon voor uitsluitend persoonlijke of huishoudelijke doeleinden niet onder de werkingssfeer van de Privacyrichtlijn en de Wbp (art. 3, tweede lid, Privacyrichtlijn en art. 2, tweede lid, onder a, Wbp).[21] Een voorbeeld hiervan is het bijhouden van een adressenbestand van vrienden en kennissen. Ook de verwerking van persoonsgegevens door een *gebruiker* van social media kan, afhankelijk van de omstandigheden van het geval, onder deze exceptie vallen.[22]

Tot slot geldt dat de materiële werkingssfeer van bepaalde delen van de Privacyrichtlijn door de lidstaten beperkt kan worden voor de verwerking van persoonsgegevens voor uitsluitend journalistieke, artistieke of literaire doeleinden, indien dit, simplistisch gesteld, nodig is om het recht op vrijheid van meningsuiting te

[20] *Kamerstukken II* 1998/99, 25892, 13, p. 2 en 3.

[21] Zie voor de reikwijdte van deze begrippen onder meer: HvJEG 6 november 2003, zaak C-101/01, ECLI:EU:C:2003:596 (*Lindqvist*) en HvJEU 11 december 2014, C-212/13, ECLI:EU:C:2014:2428 (*Ryneš*).

[22] Een aanbieder van social media is niet als een natuurlijke persoon aan te merken en kan derhalve alleen al vanwege dat gegeven geen beroep op voornoemde uitzondering doen. Een gebruiker kan berichten posten waarbij hij persoonsgegevens van zichzelf en anderen deelt, zoals foto's van of locaties waar hij en zijn vrienden zich bevinden. Veelal zal hij hiermee binnen de reikwijdte van de genoemde uitzondering blijven. Dit kan anders zijn wanneer hij er bijvoorbeeld voor kiest om zijn 'persoonlijke' Facebookprofiel in te zetten voor zakelijke doeleinden. Zie onder meer: Groep Gegevensbescherming Artikel 29, Advies 5/2009 over online sociale netwerken, *WP* 163, p. 5 en 6.

kunnen waarborgen (zie art. 9 Privacyrichtlijn). In de Wbp is dit terug te vinden in artikel 3, eerste lid, Wbp: de Wbp is slechts deels van toepassing op voornoemde verwerkingen.[23]

3.1.3 Territoriale werkingssfeer

Vestiging op het grondgebied van een lidstaat

Artikel 4 Privacyrichtlijn en artikel 4 Wbp geven de territoriale werkingssfeer weer. In de eerste plaats geldt het nationale recht van een lidstaat wanneer een persoonsgegevensverwerking wordt verricht in het kader van de activiteiten van een *vestiging* van de verantwoordelijke op het grondgebied van een lidstaat (art. 4, eerste lid, onder a, Privacyrichtlijn).

Een 'vestiging' is ieder centrum van economische activiteit. De rechtsvorm van een vestiging doet er niet toe: er kan sprake zijn van een bijkantoor zonder rechtspersoonlijkheid maar ook van een dochteronderneming met rechtspersoonlijkheid. Doorslaggevend is of er effectief en daadwerkelijk activiteiten worden uitgeoefend voor een onbepaalde periode.[24]

Voor de toepasselijkheid van het recht op grond van artikel 4, eerste lid, Wbp is evenmin van belang waar persoonsgegevens zich bevinden c.q. waar de gegevensverwerkingen (activiteiten) plaatsvinden: dit kan in de *cloud* zijn, op servers buiten Europa of op lokale servers. Gelet op de snelle technologische ontwikkelingen is ervoor gekozen om toepassing van de Privacyrichtlijn niet te laten afhangen van de plaats waar een gegevensbestand zich bevindt. De plaats van *vestiging* van de verantwoordelijke vormt het aanknopingspunt voor jurisdictie.[25] In de praktijk betekent dit dat wanneer een verantwoordelijke geen vestiging heeft in Nederland, maar wel in een van de andere landen van de Europese Unie, zoals Duitsland, dit ertoe leidt dat Duits recht moet worden toegepast op gegevensverwerkingen die zien op persoonsgegevens van Nederlandse burgers. Hoewel het Duitse en Nederlandse privacyrecht een implementatie vormen van dezelfde Privacyrichtlijn, zijn er, binnen de speelruimte die de Privacyrichtlijn biedt, wel onderlinge verschillen, zoals in de sanctionering van privacyovertredingen.

Artikel 4 Privacyrichtlijn beoogt te voorkomen dat op één en dezelfde gegevens*verwerking* het recht van meer dan een lidstaat van toepassing is. Gelet op het niveau van harmonisatie hebben lidstaten de verplichting tot wederzijds vertrouwen. Deze verplichting betekent dat één en dezelfde verwerking niet in

[23] Met name de algemene zorgvuldigheidsnormen voor het verwerken van persoonsgegevens gelden onverkort. Ook zijn de regels omtrent gedragscodes en aansprakelijkheid van toepassing, omdat deze op grond van de Privacyrichtlijn niet mogen worden uitgezonderd.

[24] *Kamerstukken II* 1998/99, 25892, 3, p. 75 (MvT) en overweging 19 Privacyrichtlijn. Voor de interpretatie kan eveneens aansluiting worden gezocht bij de uitleg die het Hof van Justitie EU aan het begrip vestiging geeft in het kader van de vrijheid van vestiging krachtens art. 50 VWEU: er is sprake van een vaste vestiging indien deze 'duurzaam over het personeel en de technische middelen beschikt die voor bepaalde diensten noodzakelijk zijn', zie HvJ EG 4 juli 1985, C-168/84, ECLI:EU:C:1985:299 (*Günter Berkholz*), r.o. 18 en 19 en HvJ EG 7 mei 1998, C-390/96, ECLI:EU:C:1998:206 (*Lease Plan Luxembourg/Belgische Staat*), r.o. 19.

[25] European Commission, Analysis and impact study on the implementation of Directive 95/46 in Member States, behorend bij het Eerste verslag over de toepassing van de Richtlijn gegevensbescherming (95/46/EG), COM(2003), 265, p. 6 en *Kamerstukken II* 1997/98, 25892, 3, p. 75.

verschillende lidstaten aan het toezicht van verschillende toezichthouders moet worden onderworpen, omdat dat het vrije verkeer van deze gegevens zou verhinderen.[26] De Privacyrichtlijn is immers een interne marktrichtlijn en artikel 4 Wbp is een van de belangrijkste bepalingen voor het bewerkstelligen van deze interne markt.[27] Tegelijkertijd moet worden gewaarborgd dat op elke gegevensverwerking *binnen* de Europese Unie het recht van één van de lidstaten van toepassing is: voorkomen moet immers worden dat iemand van de bescherming van de Privacyrichtlijn wordt uitgesloten.[28]

In de literatuur heeft een uitgebreide discussie plaatsgevonden over de uitleg van artikel 4, eerste lid, Wbp in internationale situaties waarin een verantwoordelijke vestigingen in meerdere plaatsen in of buiten de Europese Unie heeft.[29] Kernvraag daarbij was of voor de toepassing van de Wbp de verantwoordelijke *zelf* al dan niet in Nederland gevestigd moest zijn. De AP, bij monde van Fontein, nam in deze discussie het standpunt in dat wanneer een verantwoordelijke in een ander land is gevestigd en in Nederland slechts een bijkantoor of een *branch* heeft, het recht van dat andere land op gegevensverwerkingen door deze *vestiging* van toepassing was.[30] Alleen indien de verantwoordelijke *zelf* in Nederland was gevestigd, was volgens de AP de Wbp van toepassing. Hiermee werd een beperkte uitleg aan de reikwijdte van artikel 4, eerste lid, onder a, Privacyrichtlijn gegeven om cumulatie van nationale wetgeving zoveel mogelijk te voorkomen. Ter illustratie: een bedrijf is gevestigd in Duitsland en heeft een bijkantoor in Nederland. Indien de beperkte uitleg van de AP gevolgd zou worden, zou op verwerkingen door het Nederlandse bijkantoor alleen Duits recht van toepassing zijn. Maar strookte deze uitleg wel met artikel 4, eerste lid, onder a, Privacyrichtlijn? Dit artikel luidt als volgt:

> *Artikel 4 Privacyrichtlijn*
> Toepasselijk nationaal recht
> 1. Elke Lid-Staat past zijn nationale, ter uitvoering van deze richtlijn vastgestelde bepalingen toe op de verwerking van persoonsgegevens indien:
> a) die wordt verricht in het kader van de activiteiten van een vestiging op het grondgebied van de Lid-Staat van de voor de verwerking verantwoordelijke; wanneer dezelfde verantwoordelijke een vestiging heeft op het grondgebied van verscheidene Lid-Staten, dient hij de nodige maatregelen te treffen om ervoor te zorgen dat elk van die vestigingen voldoet aan de verplichtingen die worden opgelegd door de toepasselijke nationale wetgeving; (…)

Overweging 19 Privacyrichtlijn geeft de volgende toelichting:

---

[26] Mededeling van de Commissie betreffende de bescherming van personen in verband met de behandeling van persoonsgegevens in de Gemeenschap en betreffende de beveiliging van informatiesystemen, COM(90) 314 def., p. 17.

[27] Eerste verslag over de toepassing van de Richtlijn gegevensbescherming (95/46/EG), COM(2003), 265, p. 19.

[28] Zie overweging 18 Privacyrichtlijn.

[29] E.M.L. Moerel, 'Back to basics: wanneer is de Wet bescherming persoonsgegevens van toepassing?', *Computerrecht* 2008/61, p. 81-91.

[30] M.A.H. Fontein-Bijnsdorp, '"Art. 4 Wbp revisited": enkele opmerkingen inzake de toepasselijkheid van de Wet bescherming persoonsgegevens', *Computerrecht* 2008/168, p. 288. Moerel heeft in een vervolgartikel haar eigen standpunten nogmaals onderbouwd: E.M.L. Moerel, '"Art. 4 Wbp revisited"; naschrift De Nieuwe WP Opinie inzake Search Engines', *Computerrecht* 2008/169, p. 290-298.

> ‘Overwegende (...) dat, wanneer *een en dezelfde voor de verwerking verantwoordelijke gevestigd is op het grondgebied van verscheidene Lid-Staten* (eigen cursivering), met name door middel van een dochteronderneming, hij dient te waarborgen, in het bijzonder om elke vorm van wetsontduiking te voorkomen, *dat elk van de vestigingen voldoet aan de verplichtingen die het nationale recht aan de activiteiten stelt* (eigen cursivering); (…)’

In de Wbp is artikel 4, eerste lid, onder a, Privacyrichtlijn als volgt geïmplementeerd:

> *Artikel 4 Wbp*
> 1. Deze wet is van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten van een vestiging van een verantwoordelijke in Nederland.

Noch uit artikel 4, eerste lid, onder a, Privacyrichtlijn, noch uit artikel 4, eerste lid, Wbp kan worden afgeleid dat de verantwoordelijke *zelf* in de lidstaat gevestigd moet zijn om het nationale recht van die lidstaat van toepassing te laten zijn: de aanwezigheid van een vestiging die in het kader van de activiteiten van die vestiging persoonsgegevens verwerkt in een bepaalde lidstaat, *triggert* reeds de toepasselijkheid van het recht van die lidstaat. Of de verantwoordelijke zelf dan in die lidstaat gevestigd is of in een andere lidstaat en aldaar aan het geldende nationale recht is onderworpen, doet niet ter zake. De Wbp kan dan van toepassing zijn als een verantwoordelijke in Duitsland gevestigd is en een bijkantoor heeft in Nederland, waarbij persoonsgegevens worden verwerkt in het kader van de activiteiten van de Nederlandse vestiging.

In de Privacyrichtlijn is namelijk niet gekozen voor een *land-van-oorsprongbeginsel* waarbij alleen de wet van het (oorspronkelijke) land waar de verantwoordelijke is gevestigd geldt: als de verantwoordelijke zich via meerdere vestigingen ook vestigt in andere landen en gegevensverwerkingen vinden plaats in het kader van de activiteiten van de vestigingen in die lidstaten, dan zal het nationale privacyrecht van die lidstaten ook van toepassing zijn.[31]

Een beperkte uitleg van artikel 4, eerste lid, onder a, Privacyrichtlijn, waarbij de verantwoordelijke *zelf* in een lidstaat gevestigd zou moeten zijn om het recht van die lidstaat van toepassing te laten zijn, kan tot lacunes in de rechtsbescherming leiden. Zo zou een Amerikaanse bedrijf met één of meerdere vestigingen die in Europa persoonsgegevens van Europese burgers verwerken, niet aan het nationale recht van een van de lidstaten zijn onderworpen, omdat de verantwoordelijke zelf buiten de Europese Unie gevestigd is. Ook kan geen beroep worden gedaan op artikel 4, eerste lid, onder c, Privacyrichtlijn. Dit artikel zal hierna uitgebreider uiteen worden gezet, maar komt er kort gezegd op neer dat wanneer een verantwoordelijke *geen* vestiging heeft in de Europese Unie, maar hier wel gebruikmaakt van middelen voor de gegevensverwerking, alsnog het nationale recht van het land waar deze middelen zich bevinden, van toepassing is.

Sinds december 2010 lijkt de AP ook van de ruimere territoriale werkingssfeer van artikel 4, eerste lid, Wbp uit te gaan: de Wbp is van toepassing als persoonsgegevens worden verwerkt in het kader van de activiteiten van een vestiging van de verantwoordelijke in Nederland. Dit vermoeden volgt uit het feit dat

[31] G.J. Zwenne & G.C.J. Erents, ‘Reikwijdte Wbp: enige opmerkingen over de uitleg van art. 4, eerste lid, Wbp’, *Privacy & Informatie* 2009/2, p. 65.

de AP betrokken is geweest bij de totstandkoming van een Europees advies over toepasselijk recht dat uitgaat van de ruime territoriale werkingssfeer van de Privacyrichtlijn.[32] Dit advies, dat verderop in dit preadvies uitgebreider besproken zal worden, is opgesteld door de Groep Gegevensbescherming Artikel 29 (ook wel de 'Artikel 29 Werkgroep' genoemd), het onafhankelijke adviesorgaan van de Europese Commissie inzake gegevensbescherming en de persoonlijke levenssfeer. De Artikel 29 Werkgroep bestaat uit vertegenwoordigers van de nationale toezichthouders, een vertegenwoordiger van de Europese Commissie en de European Data Protection Supervisor, die toezicht houdt op de verwerking van persoonsgegevens door de communautaire instellingen. De Artikel 29 Werkgroep werd op dat moment voorgezeten door de toenmalige voorzitter van de AP, Jacob Kohnstamm. Dit impliceert dat de AP haar standpunt dat de verantwoordelijke zelf in Nederland gevestigd moet zijn om de Wbp op een gegevensverwerking van toepassing te verklaren, in december 2010 heeft verlaten. Een bevestiging van het vermoeden dat de AP inderdaad inmiddels van deze ruimere uitleg uitgaat, is terug te vinden in een onderzoek naar Google Inc. uit november 2013.[33] In deze zaak onderzocht de AP de gewijzigde privacyvoorwaarden van Google Inc. waarin Google Inc. aankondigde de persoonsgegevens die zij van gebruikers van verschillende Google-diensten verzamelde, te gaan combineren en te gebruiken voor andere diensten.[34] Hieronder vielen ook de gegevens die Google Inc. verzamelde wanneer websitehouders gebruikmaken van bepaalde *cookies* van Google Inc., zoals Google Analytics. Google Inc. verschafte hierover geen adequate informatie en vroeg evenmin toestemming aan internetgebruikers. Google Inc. verzamelt en combineert de gegevens onder meer voor het tonen van gepersonaliseerde advertenties.
Google Inc. heeft een vestiging in Nederland, Google Netherlands B.V. Google Inc. biedt haar diensten veelal gratis aan en is daarom afhankelijk van reclame-inkomsten. Google Netherlands B.V. houdt zich met name bezig met het verkopen van advertenties aan Nederlandse adverteerders en ook is er een Nederlandse website. De Nederlandse vestiging vormt een essentiële schakel naar de Nederlandse advertentiemarkt. Simpel gezegd: door de gegevensverwerking kan Google Netherlands B.V. meer advertenties verkopen. De AP meent daarom dat de gevensverwerking – het verzamelen en combineren van persoonsgegevens door Google Inc. – plaatsvond in het kader van de activiteiten van Google Netherlands B.V. en dat de Wbp derhalve van toepassing is.[35] Naar aanleiding van de uitkomsten van dit onderzoek heeft de AP besloten om tot handhaving over te gaan en legt zij Google Inc. in november 2014 een last onder dwangsom op.[36] Tussen de publicatie van het onderzoek en het moment waarop de last werd opgelegd, had het Hof van Justitie EU inmiddels uitspraak gedaan in een soortgelijke Spaanse zaak, bekend als het G*oogle Spain*-arrest, waarin de ruime uitleg van de territoriale werkingssfeer eveneens is bevestigd.[37] Deze zaak wordt

[32] Groep Gegevensbescherming Artikel 29, Advies 8/2010 over toepasselijk recht, goedgekeurd op 16 december 2010, *WP* 179, p. 20.

[33] College bescherming persoonsgegevens, Onderzoek naar het verwerken van persoonsgegevens door Google, november 2013, *z*2013-00194.

[34] Dit onderzoek was een vervolgstap op een gezamenlijk onderzoek van de Artikel 29 Werkgroep in 2012 naar deze voorwaarden, zie de brief aan Google Inc. van de Artikel 29 Werkgroep d.d. 16 oktober 2012, te raadplegen via: www.cnil.fr/sites/default/files/typo/document/20121016-letter_google-article_29-FINAL.pdf.

[35] Zie noot 33, p. 39-41.

[36] College bescherming persoonsgegevens, Last onder dwangsom Google Inc., 17 november 2014, *z*2014-00038.

[37] HvJ EU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain/Costeja*). De AP refereert in randnummer 18 van de last onder dwangsom aan dit arrest.

uitgebreid besproken in paragraaf 4.1. Recentelijk maakte de AP bekend dat Google Inc. inmiddels alle geconstateerde overtredingen heeft beëindigd.[38]
Dat de AP haar rechtsmacht erkent, ook wanneer de verantwoordelijke niet zelf in Nederland is gevestigd, is uiteraard een goede zaak, omdat mogelijke lacunes in de rechtsbescherming hierdoor worden ondervangen. Inmiddels is deze lijn voortgezet in een nog lopend onderzoek dat de AP in december 2014 is gestart naar de gewijzigde privacyvoorwaarden van Facebook Inc.[39] en in een onlangs afgerond onderzoek naar de verwerking van persoonsgegevens door Nike Inc. in het kader van de *Nike+ Run Club*-app.[40] In beide zaken wordt nadrukkelijk verwezen naar het *Google Spain*-arrest om bevoegdheid voor de AP te creëren.[41] Het is een gemiste kans dat de AP voor 2013 geen gebruik heeft gemaakt van de rechtsmacht die haar is toegekend. Een kritische kanttekening die hierbij kan worden geplaatst, is dat de AP haar standpuntswijziging niet duidelijk heeft gecommuniceerd, maar dat dit uit onderzoeken en een persbericht[42] over het advies van de Artikel 29 Werkgroep moet worden afgeleid. Op de website van de AP wordt in de 'Wbp-naslag'[43], de officieuze tekst en commentaar bij de Wbp, geen duidelijkheid verschaft. Daarnaast staat op de website (nog altijd) het artikel van Fontein gepubliceerd.[44] Het zou de rechtszekerheid ten goede komen wanneer de AP het artikel van haar website verwijdert en de 'Wbp-naslag' op dit punt verduidelijkt. Ook in diverse richtsnoeren die door de AP zijn uitgegeven, die vaak schema's bevatten om te bepalen of de Wbp van toepassing is, is meer toelichting wenselijk. Dit temeer omdat, zoals ook uit de hierna in paragraaf 4 behandelde Europese arresten blijkt, het bepalen van de rechtsmacht een complexe aangelegenheid is.

Volledigheidshalve dient nog te worden opgemerkt dat er nog een situatie is waarin meer dan één nationaal recht van toepassing kan zijn op een gegevensverwerking. Indien een verantwoordelijke in Nederland een bewerker in Duitsland inschakelt, dient de verantwoordelijke er op grond van artikel 17, derde lid, Privacyrichtlijn jo. artikel 14, vierde lid, Wbp op toe te zien dat de bewerker voldoet aan de beveiligingsverplichtingen en de eisen die er op grond van een mogelijke meldplicht aangaande datalekken gelden onder de Duitse privacywetgeving. Deze specifieke situatie zal in het vervolg van dit preadvies buiten beschouwing worden gelaten.

---

[38] Autoriteit Persoonsgegevens, Overtredingen Google beëindigd na optreden Autoriteit Persoonsgegevens, persbericht 14 juni 2016, te raadplegen via: https://autoriteitpersoonsgegevens.nl/nl/nieuws/overtredingen-google-be%C3%ABindigd-na-optreden-autoriteit-persoonsgegevens.

[39] College bescherming persoonsgegevens, Cbp onderzoekt nieuwe privacyvoorwaarden Facebook, persbericht 16 december 2014, te raadplegen via: https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-onderzoekt-nieuwe-privacyvoorwaarden-facebook.

[40] College bescherming persoonsgegevens, Onderzoek naar de verwerking van persoonsgegevens in het kader van de Nike+ Running-app door Nike Inc., z2014-00859.

[41] Zie noot 39 en zie noot 40, p. 39-41.

[42] College bescherming persoonsgegevens, Privacytoezichthouders verhelderen regels voor toepasselijk Privacyrecht, nieuwsbericht 7 januari 2011, te raadplegen via: https://autoriteitpersoonsgegevens.nl/nl/nieuws/privacytoezichthouders-verhelderen-regels-voor-toepasselijk-privacyrecht.

[43] Te raadplegen via: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wbp-naslag.

[44] Zie: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/th_dossier/285-289.pdf.

Het gebruikmaken van middelen op het grondgebied van een lidstaat

In de tweede plaats kan rechtsmacht ontstaan indien de verantwoordelijke geen vestiging heeft binnen de Europese Unie, maar voor de verwerking van persoonsgegevens gebruikmaakt van al dan niet geautomatiseerde *middelen* die zich op het grondgebied van een lidstaat bevinden. De feitelijke gegevensverwerking vindt dan in de Europese Unie plaats. Bij middelen kan worden gedacht aan servers en telecommunicatieapparatuur, maar ook aan het verzamelen van persoonsgegevens door middel van *cookies* of javascripts die zich op smartphones of tablets bevinden.[45] De middelen hoeven derhalve niet in het bezit te zijn van de verantwoordelijke maar kunnen ook aan een betrokkene toebehoren. Het criterium 'middelen' wordt ruim uitgelegd: het feit dat een persoon enquêtes of vragenlijsten afneemt, kan worden aangemerkt als het gebruik van een middel.[46] Bij het gebruik van middelen op het grondgebied van een lidstaat is het recht van die lidstaat van toepassing, tenzij deze middelen slechts voor doorvoer worden gebruikt, bijvoorbeeld omdat de gegevens nu eenmaal door een internetkabel op het grondgebied lopen (art. 4, eerste lid, onder c, Privacyrichtlijn en art. 4, tweede lid, Wbp). Indien de verantwoordelijke gebruikmaakt van al dan niet geautomatiseerde middelen in een lidstaat, dient hij een vertegenwoordiger op het grondgebied van de lidstaat aan te stellen (art. 4, eerste lid, onder c, Privacyrichtlijn). Dit is terug te vinden in artikel 4, derde lid, Wbp, waarin is bepaald dat het voor een verantwoordelijke verboden is om persoonsgegevens te verwerken, indien hij geen vertegenwoordiger aanstelt.[47] Deze vertegenwoordiger kan een persoon of een instantie zijn en handelt namens de verantwoordelijke in overeenstemming met de Wbp. Voor de toepassing van de Wbp wordt de vertegenwoordiger aangemerkt als de verantwoordelijke. Dit laat overigens onverlet dat rechtsvorderingen ook tegen de verantwoordelijke zelf kunnen worden ingesteld.

De toepasselijkheid van de Nederlandse Wbp op grond van artikel 4, tweede lid, Wbp kan worden geïllustreerd aan de hand van twee onderzoeken van de AP.

In 2013 startte de AP een onderzoek naar vermoedelijke privacyschendingen door Whatsapp Inc., de aanbieder van de populaire instant messaging app whatsapp.[48,49] Het bleek namelijk dat gebruikers om whatsapp te kunnen gebruiken, WhatsApp Inc. toegang dienden te geven tot hun volledige adresboek. Op die manier kon WhatsApp Inc. zien welke contacten al whatsapp gebruikten en welke niet. Ook de gegevens van niet-gebruikers werden door WhatsApp Inc. opgeslagen. Dit was niet nodig om te kunnen whatsappen en de gegevens van talloze niet-gebruikers kwamen zo zonder hun medeweten in handen van WhatsApp Inc. Tevens werden de whatsappberichtjes onversleuteld verzonden, waardoor zij door anderen konden worden onderschept. Bovendien was de methode waarop WhatsApp Inc. wachtwoorden aanmaakte, niet veilig en werden de persoonsgegevens van whatsapp-gebruikers te lang bewaard.

---

[45] Zie noot 32, p. 20.

[46] *Ibid.*, p. 23.

[47] Het niet aanwijzen van een vertegenwoordiger is een van de twee bepalingen die op grond van art. 75 Wbp strafrechtelijk kan worden gesanctioneerd.

[48] College bescherming persoonsgegevens, Onderzoek naar de verwerking van persoonsgegevens in het kader van de mobiele applicatie whatsapp door WhatsApp Inc., 28 januari 2013, z2011-00987.

[49] Dit onderzoek naar WhatsApp Inc. is bijzonder omdat het het eerste onderzoek is waarbij op trans-Atlantisch niveau is samengewerkt. Het onderzoek werd namelijk uitgevoerd samen met de Canadese privacytoezichthouder, de Office of the Privacy Commissioner of Canada.

Duidelijk was dat WhatsApp Inc. op grote schaal persoonsgegevens verwerkte van miljoenen Nederlandse gebruikers én niet-gebruikers, zoals telefoonnummers, de inhoud van whatsappberichtjes (foto's, locatiegegevens e.d.) en statusberichten e.d. De vraag was echter of de AP ter zake rechtsmacht toekwam. WhatsApp Inc. had ten tijde van het onderzoek geen kantoren buiten de Verenigde Staten. De AP diende aan te tonen dat de verwerking van persoonsgegevens door WhatsApp Inc. toch binnen het toepassingsbereik van het Nederlandse privacyrecht viel. De AP redeneerde als volgt. WhatsApp Inc. gebruikt de smartphones van Nederlandse whatsapp-gebruikers als middel voor de verwerking van persoonsgegevens via de app. De middelen worden niet slechts voor de doorvoer van persoonsgegevens gebruikt: WhatsApp Inc. richt zich (mede) op Nederlandse gebruikers. Dit is af te leiden uit de Nederlandse dialoogboxen (zoals instellingsschermen) en overige informatie die in het Nederlands beschikbaar is.[50] Hiermee is volgens de AP de toepasselijkheid van de Wbp gegeven. Het feit dat WhatsApp Inc. via haar voorwaarden en Privacy Notice contractueel de toepassing van een ander recht dan het recht van Californië uitsloot, doet niets af aan de toepasselijkheid van de Wbp. De Wbp is dwingend recht; de toepasselijkheid kan niet via een eenzijdige verklaring of contractueel worden uitgesloten.

Ondanks het feit dat WhatsApp Inc. gedurende het gehele onderzoek de bevoegdheid van de AP is blijven betwisten, heeft zij inmiddels meerdere maatregelen genomen om de geconstateerde overtredingen te beëindigen. Eén overtreding is echter nog altijd niet beëindigd: Whatsapp Inc. had, bij gebrek aan een vestiging in de Europese Unie, in Nederland een vertegenwoordiger moeten aanwijzen. De AP besloot daarom een last onder dwangsom op te leggen van € 10.000 per dag met een maximum van € 1.000.000.[51] Whatsapp Inc. heeft hiertegen bezwaar gemaakt en nadat dit bezwaar is afgewezen, beroep ingesteld, maar ook dat beroep is recentelijk ongegrond verklaard.[52] In beroep voerde Whatsapp Inc. onder meer aan dat het in de praktijk onmogelijk is om een vertegenwoordiger te vinden, omdat deze aansprakelijkheid op zich moet nemen voor boetes en dwangsommen die Whatsapp Inc. kan oplopen, terwijl de lokale vertegenwoordiger geen enkele invloed heeft op de activiteiten van Whatsapp Inc. De rechter heeft evenwel geoordeeld dat partijen dit contractueel kunnen afdichten (zie r.o. 5.3 en 11). Whatsapp Inc. ontkomt er dus niet aan om een vertegenwoordiger in Nederland aan te stellen.

Een ander voorbeeld is het onderzoek van de AP naar de verzameling van allerlei persoonsgegevens door Google Inc.[53] voor de dienst *Google Street View*. Via *Google Street View* kunt u precies zien of het huis waarover uw collega zo opschept een rijtjeshuis is of, zoals hij zegt: 'een luxueuze schakelvilla'. Ook is het uiteraard handig om van tevoren op te kunnen zoeken hoe een adres dat u moet bezoeken er aan de buitenkant uitziet. Om Nederland in kaart te brengen liet Google Inc. gedurende twee jaar speciaal daartoe met camera's uitgeruste Streetview-auto's door de Nederlandse straten rijden. Naast camera's hadden de auto's ook apparatuur aan boord om draadloos internetverkeer op te vangen. Met deze apparatuur werd gedurende twee jaar informatie verzameld, waaronder MAC-adressen van 3,6 miljoen routers die aanstonden op het moment dat de Street View-auto langsreed. Simplistisch gezegd kon Google Inc. hierdoor de foto's aan een exacte locatie koppelen. Ook werden inhoudelijke communicatiegegevens van

[50] Zie voor de link met de toepasselijkheid van art. 11.7a Tw en de daarin opgenomen verplichting om toestemming te verkrijgen van de niet-gebruikers van whatsapp paragraaf 3.6 van het onderzoek.
[51] College bescherming persoonsgegevens, Last onder dwangsom WhatsApp Inc., 22 juli 2014, niet gepubliceerd.
[52] Rb. Den Haag 22 november 2016, ECLI:NL:RBDHA:2016:14088.
[53] College bescherming persoonsgegevens, Onderzoek naar de verzameling van Wifi-gegevens met Street View auto's door Google, 7 december 2010, *z*2010-00582.

onbeveiligde draadloze WiFi-netwerken opgevangen. Google Inc. had de eigenaren van de routers hier niet over geïnformeerd en had ook geen grondslag (zoals toestemming of een gerechtvaardigd belang in de zin van art. 8 Wbp) voor deze gegevensverwerking. Ook op andere punten voldeed Google Inc. niet aan de Wbp. De AP besloot dan ook op te treden en stelde zich op het standpunt dat de Wbp van toepassing was, omdat Google Inc. 'middelen', namelijk de met apparatuur uitgeruste Street View-auto's, inzette om persoonsgegevens te verwerken.[54] Over het feit dat Google Inc. wel een vestiging heeft in Nederland ten tijde van het onderzoek, te weten Google Netherlands B.V., merkt de AP in deze zaak slechts op dat dit de lokale vertegenwoordiger is van Google Inc. Een nadere uitleg van diens activiteiten of het vaststellen dat dit een 'irrelevante' vestiging betreft waardoor een beroep op artikel 4 lid 2 Wbp mogelijk is, blijft achterwege. Uiteindelijk legde de AP Google Inc. een last onder dwangsom van € 1 miljoen op.[55]

Advies 8/2010 inzake toepasselijk recht

Niet alleen in Nederland, maar ook in de andere lidstaten werd geworsteld met de uitleg van artikel 4 van de Richtlijn. Zoals hierboven reeds kort is aangehaald, publiceerde de Artikel 29 Werkgroep in december 2010 een uitgebreid advies gericht op de uitleg van de territoriale werkingssfeer van de Privacyrichtlijn en de gevolgen daarvan voor de toepassing van nationale privacywetgeving.[56]

De Artikel 29 Werkgroep gaat uit van een ruime territoriale werkingssfeer van de Privacyrichtlijn, die niet alleen tot het Europese territoir beperkt is. Indien persoonsgegevens *buiten* de Europese Unie worden verwerkt in het kader van de activiteiten van een vestiging van een verantwoordelijke *in* de Europese Unie, is de Privacyrichtlijn van toepassing. De plaats van de gegevensverwerking is immers niet doorslaggevend. Dit is temeer van belang nu deze plaats mede door technologische ontwikkelingen, zoals *cloud computing*, steeds moeilijker te bepalen is.[57] Indien een verantwoordelijke *buiten* de Europese Unie gevestigd is, maar middelen voor het verwerken van persoonsgegevens gebruikt die zich *binnen* de Europese Unie bevinden, is de Privacyrichtlijn eveneens van toepassing.[58] De nationaliteit, de verblijfplaats van de betrokkenen en de fysieke locatie van de persoonsgegevens spelen geen rol.[59]

Voor de toepassing van artikel 4, eerste lid, onder a, Privacyrichtlijn kiest de Artikel 29 Werkgroep voor de ruime uitleg: de aanwezigheid van een vestiging van de voor de verwerking verantwoordelijke in een lidstaat leidt in beginsel tot de toepassing van het recht van die lidstaat. De aanwezigheid van vestigingen in andere lidstaten kan dus tot gevolg hebben dat ook het nationale recht van die andere lidstaten van toepassing is. Om te bepalen welk nationale recht van toepassing is, is de invulling van het begrip '*in het kader van de activiteiten*' van de vestiging doorslaggevend, waarbij de vestiging de gegevens niet zelf hoeft te verwerken. Beoordeeld moet worden of de vestiging betrokken is bij activiteiten die verband houden met

[54] Over het feit dat Google Inc. wel een vestiging heeft in Nederland ten tijde van het onderzoek, te weten Google Netherlands B.V., merkt de AP slechts op dat dit de lokale vertegenwoordiger is van Google Inc. Een nadere uitleg van diens activiteiten of het vaststellen dat dit een 'irrelevante' vestiging betreft waardoor een beroep op art. 4 lid 2 Wbp mogelijk is, blijft achterwege.
[55] College bescherming persoonsgegevens, Last onder dwangsom, 23 maart 2011, z2010-01467.
[56] Zie noot 32.
[57] *Ibid.*, p. 7.
[58] *Ibid.*, p. 9.
[59] *Ibid.*, p. 9 en 10.

de gegevensverwerking. Elementen die daarbij een rol spelen zijn (1) de mate van betrokkenheid bij de activiteiten in het kader waarvan persoonsgegevens worden verwerkt; (2) de aard van de activiteiten; en (3) de noodzaak om een doeltreffende gegevensverwerking te waarborgen. De rechtsvorm van de vestiging is niet doorslaggevend: zelfs de aanwezigheid van een agent in een lidstaat kan als een relevante vestiging van een verantwoordelijke worden beschouwd indien zijn aanwezigheid voldoende duurzaam is.[60] De Artikel 29 Werkgroep vat het als volgt samen:

> 'De doorslaggevende factoren zijn de aard en plaats van de gewone activiteiten die worden verricht en die het "kader" vormen waarin de verwerking wordt verricht.'[61]

Ten aanzien van artikel 4 eerste lid, onder c, Privacyrichtlijn legt de Artikel 29 Werkgroep uit dat de Privacyrichtlijn de cumulatieve toepassing van artikel 4, eerste lid, onder a, en artikel 4, eerste lid, onder c, Privacyrichtlijn uitsluit.[62] Indien een verantwoordelijke een vestiging heeft in de Europese Unie en een gegevensverwerking plaatsvindt in het kader van de activiteiten van die vestiging, is het nationale recht van het land van die vestiging van toepassing. Het feit dat zich in andere landen ook middelen voor het verwerken van persoonsgegevens bevinden, is irrelevant. De verwerkingen worden immers verricht in het kader van de activiteiten van de vestiging.

Maar wat nu als een verantwoordelijke *wel* een vestiging heeft binnen de Europese Unie, maar deze vestiging niet betrokken is bij de gegevensverwerking en de verantwoordelijke wel middelen gebruikt in de Europese Unie om persoonsgegevens te verzamelen? In dat geval moet men doen alsof er geen vestiging is binnen de Europese Unie en kan artikel 4, eerste lid, onder c, Privacyrichtlijn worden toegepast, teneinde een lacune in de rechtsbescherming te voorkomen.[63] De Artikel 29 Werkgroep licht toe dat de ruime uitleg van het criterium 'middelen' als ongewenst bijeffect heeft dat de Privacyrichtlijn van toepassing is op gegevensverwerkingen die nauwelijks een band met de EU hebben. Een Amerikaanse partij die gegevens van Amerikanen verwerkt via de databases van een bewerker in Frankrijk, wordt in dat geval immers onderworpen aan Frans privacyrecht.[64]

Ook merkt de Artikel 29 Werkgroep op dat het toepasselijke recht niet altijd samen hoeft te vallen met de bevoegdheid van een nationale rechter. De Richtlijn laat de nationale bepalingen omtrent de rechterlijke bevoegdheid onverlet. Dat het niet adequaat regelen daarvan in de praktijk grote consequenties kan hebben ten aanzien van de mogelijkheden om een partij in rechte aan te spreken, wordt nader uitgewerkt in paragraaf 4.4.

De belangrijkste conclusies van de Artikel 29 Werkgroep zijn dan ook niet verrassend: de tekst van artikel 4 Privacyrichtlijn zou duidelijker kunnen, onder meer door te verduidelijken wat er bedoeld wordt met 'in het kader van de activiteiten van een vestiging' en door aan te geven dat indien er geen 'relevante' vestiging is binnen de EU, een beroep op artikel 4, eerste lid, onder c, Privacyrichtlijn mogelijk is. Om de cumulatie

---

[60] *Ibid.*, p. 14 en 22. Zie ook: Groep Gegevensbescherming Artikel 29, Advies 1/2008 over gegevensbescherming en zoekmachines, goedgekeurd op 4 april 2008, *WP* 148, p. 10 en 11.
[61] Zie noot 32, p. 18.
[62] *Ibid.*, p. 33 en 34.
[63] *Ibid.*, p. 23.
[64] *Ibid.*, p. 24.

van nationale wetgeving te voorkomen, zou kunnen worden overwogen om terug te keren naar het *land-van-oorsprong-beginsel*, waarbij het recht van het land waar de hoofdvestiging van de verantwoordelijke zich bevindt, zou gelden voor alle vestigingen, ongeacht waar die zich bevinden. Daarvoor is het echter noodzakelijk dat de nationale privacywetgeving verder wordt geharmoniseerd. Zo lopen momenteel de sancties per lidstaat enorm uiteen. Het onverkort toepassen van het *land-van-oorsprong-beginsel* zou dan kunnen leiden tot *forum shopping*, waarbij verantwoordelijken zich vestigen in landen waar minder strikt tegen schendingen van de nationale privacywetgeving wordt opgetreden.[65] De AP heeft in het verleden aangegeven dat zij een *land-van-oorsprong-beginsel* afwijst. Zij meent dat, hoewel er vanuit het oogpunt van lastenverlichting en het vrije verkeer van persoonsgegevens iets voor te zeggen is, toepassing van dit beginsel nadelig is voor de betrokkene, omdat het voor hem moeilijker wordt om de bescherming van zijn privacy af te dwingen. [66]

De Artikel 29 Werkgroep geeft tevens aan dat, indien de verantwoordelijke buiten de EU gevestigd is, maar er wel een duidelijke band is met de EU, er gekeken moet worden of het Europese recht ook van toepassing kan zijn als een verantwoordelijke duidelijk zijn diensten richt op personen in de EU, bijvoorbeeld door informatie in bepaalde talen op zijn website aan te bieden of door producten te versturen naar de EU.[67] Deze norm kennen we uit het consumentenrecht.[68] Een kanttekening die ik hierbij wil maken, is de volgende. Deze aanbeveling lijkt haaks te staan op de ruime uitleg van het begrip 'middelen' die door de Artikel 29 Werkgroep gepropageerd wordt. Zou men immers niet al kunnen zeggen dat wanneer een bedrijf een webshop heeft, de gegevensverwerking plaatsvindt via computers of smartphones die zich in een lidstaat bevinden, zoals door de AP in de WhatsApp-zaak wordt betoogd? De Artikel 29 Werkgroep lijkt deze discrepantie ook te zien: artikel 4, eerste lid, onder c, Privacyrichtlijn zou alleen nog als restbepaling dienen te worden gehanteerd, voor de gevallen waarin de verantwoordelijke geen vestiging in de EU heeft en ook onvoldoende kan worden aangetoond dat de verantwoordelijke zich op de EU richt.

Verderop in dit preadvies zal worden bezien in hoeverre de conclusies en aanbevelingen van de Artikel 29 Werkgroep zijn overgenomen in de nieuwe Europese Privacyverordening.

Overige aandachtspunten

Volledigheidshalve wordt nog opgemerkt dat het ook zo kan zijn dat de verantwoordelijke niet op het grondgebied van de lidstaat gevestigd is, maar op een plaats waar de nationale wet op grond van het internationale publiekrecht van toepassing is (art. 4, eerste lid, onder b, Privacyrichtlijn). Zo is Nederlands recht van toepassing op Nederlandse schepen, vliegtuigen en op Nederlandse ambassades en diplomatieke vertegenwoordigingen. Tot slot dient te worden vermeld dat de Privacyrichtlijn de territorialiteitsregels inzake het strafrecht onverlet laat.[69]

---

[65] *Ibid.*, p. 35.

[66] Zie noot 30, p. 289.

[67] Zie noot 32, p. 36.

[68] HvJ EU 7 december 2010, gevoegde zaken C-585/08 (*Pammer*) en C-144/09 (*Hotel Alpenhof*). Zie hierover eveneens het preadvies van R.E. Tak en R. Klein, Over de grens gaan: grensoverschrijdende handhaving van het mededingings- en consumentenrecht.

[69] Zie overweging 21 Privacyrichtlijn.

3.2 Toezicht

Op grond van artikel 28 Privacyrichtlijn dient elke lidstaat een of meer onafhankelijke autoriteiten te belasten met het toezicht op de naleving van de Privacyrichtlijn. Deze autoriteiten dienen te worden geraadpleegd bij het opstellen van privacyrechtelijke wet- en regelgeving (zie art. 28, tweede lid, Privacyrichtlijn jo. art. 51, tweede lid, Wbp). De autoriteiten dienen te beschikken over onderzoeksbevoegdheden en effectieve handhavingsbevoegdheden. Ook moeten zij de bevoegdheid hebben om in rechte te kunnen optreden bij inbreuken op nationale wetgeving (waarin de Privacyrichtlijn is geïmplementeerd) of om deze inbreuken onder de aandacht van de rechterlijke instanties te brengen (zie art. 28, derde lid, Privacyrichtlijn jo. m.n. art. 60 en 61 Wbp). In Nederland is dit toezicht bij de AP belegd (zie art. 51, eerste lid jo. artikel 61, eerste lid, Wbp).

Deze bevoegdheden mogen door elke toezichthouder worden uitgeoefend op het eigen grondgebied, *ongeacht welk recht van toepassing* is (zie art. 28, zesde lid, Privacyrichtlijn jo. art. 51, eerste lid, tweede zin, Wbp). Toepasselijk recht en toezichtsbevoegdheid vallen derhalve niet altijd samen. Bij toezicht op 'vreemd' recht gelden echter wel beperkingen, welke in paragraaf 4.2 nader worden toegelicht.

De autoriteiten kunnen elkaar ook verzoeken hun bevoegdheden uit te oefenen. Zij zijn verplicht om samen te werken als dat nodig is ter uitvoering van hun taken, bijvoorbeeld via het verstrekken van inlichtingen (zie art. 61, zesde lid, Wbp). Hiertoe zijn zij ook op grond van het beginsel van loyale samenwerking ex artikel 4, derde lid van het Verdrag betreffende de Europese Unie verplicht. Dit betekent echter niet dat de ene lidstaat de andere lidstaat kan dwingen tot het starten van een onderzoek naar een gegevensverwerking door een verantwoordelijke die vanuit een vestiging op het grondgebied van laatstgenoemde lidstaat plaatsvindt.

In de praktijk betekent dit dat ondernemingen de *verantwoordelijkheid* voor een bepaalde gegevensverwerking kunnen overhevelen naar een entiteit in een andere lidstaat, om zo aan het privacyrecht en het sanctionerende toezicht in een bepaalde lidstaat te 'ontsnappen'. Dit werd pijnlijk duidelijk in een recent onderzoek van de AP. De AP startte in 2011 een onderzoek naar YD Display Advertising Benelux B.V. (YD).[70] YD plaatste zogenoemde *tracking cookies*,[71] waarmee ze het surfgedrag van internetgebruikers op websites van haar adverteerders kon volgen en vervolgens op andere websites die de gebruiker bezocht, advertenties van haar adverteerders kon tonen. Versimpeld: u zoekt een uurtje naar nieuwe schoenen op *Zalando* en als u vervolgens op *nu.nl* het nieuws leest, ziet u overal aanbiedingen van precies die zwarte schoenen die u vaak heeft aangeklikt. Voor het plaatsen van dergelijke *cookies* is naar Nederlands recht ondubbelzinnige geïnformeerde toestemming van de internetgebruikers nodig, bijvoorbeeld via een *cookie banner* waarin informatie wordt verschaft en waarin u moet aanklikken dat u akkoord gaat met het plaatsen en uitlezen van deze *cookies*. De AP besloot om aan YD een last onder dwangsom op te leggen. YD had echter intussen de verantwoordelijkheid voor de verwerking van de persoonsgegevens verplaatst naar haar vestiging in het Verenigd Koninkrijk. De AP heeft geen rechtsmacht

[70] College bescherming persoonsgegevens, Onderzoek naar de verwerking van persoonsgegevens door YD voor behavioural targeting, 27 maart 2011, gecorrigeerd op 29 april 2014, *z*2012-00811 en College bescherming persoonsgegevens, Last onder dwangsom, 17 april 2015, gepubliceerd op 19 januari 2016, *z*2014-00387.
[71] Zie noot 19.

in het Verenigd Koninkrijk, omdat op de gegevensverwerking Engels recht van toepassing is geworden. De AP heeft daarop contact gezocht met de Engelse privacytoezichthouder, maar die heeft aangegeven dat hij, gelet op de verschillen tussen het Engelse en Nederlandse privacyrecht, geen mogelijkheid ziet om op te treden.

Momenteel zijn diverse prejudiciële vragen bij het Hof van Justitie van de EU aanhangig waarin wordt verzocht om meer duidelijkheid over de toezichtsbevoegdheden en de samenwerkingsverplichtingen bij toezicht op multinationals met meerdere vestigingen in de Europese Unie.[72] Met name de situatie waarin een concern in de Europese Unie meerdere vestigingen met verschillende taken heeft, roept vragen op. Wat zijn bijvoorbeeld de rollen van de verschillende toezichthouders indien een concern in lidstaat A een verantwoordelijke heeft die volgens het concernbeleid exclusief verantwoordelijk is voor de verwerking van persoonsgegevens in de hele Europese Unie, maar ook een vestiging heeft in lidstaat B die activiteiten verricht die zich specifiek op lidstaat B richten? Ongeacht welk recht van toepassing is, mag een toezichthouder immers ook de bevoegdheden die hij op grond van artikel 28, derde lid, Privacyrichtlijn heeft, uitoefenen binnen zijn grondgebied (zie art. 28, zesde lid, Privacyrichtlijn). Mag de toezichthouder in lidstaat B autonoom optreden tegen de verantwoordelijke in lidstaat A? Of is hij verplicht om eerst de toezichthouder in lidstaat A te vragen om op te treden? Het zal interessant zijn om te zien of het Hof de samenwerkingsverplichting van de toezichthoudende autoriteiten al dan niet verder specificeert.

Volledigheidshalve zij nog opgemerkt dat momenteel in het algemeen geldt dat in de situatie waarin een nationale privacytoezichthouder wel rechtsmacht heeft en besluit een bestuurlijke boete op te leggen aan een partij die in een andere lidstaat of buiten de EU is gevestigd, hij veelal weinig mogelijkheden heeft om daadwerkelijk tot inning van een dergelijke boete over te gaan.[73]

[72] Verzoek om een prejudiciële beslissing ingediend door het Bundesverwaltungsgericht (Duitsland) op 14 april 2016 – Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein / Wirtschaftsakademie Schleswig-Holstein GmbH, C-210/16, te raadplegen via http://curia.europa.eu/.

[73] Zie voor een uitgebreide uiteenzetting van deze problematiek in het WODC-rapport van A.J. Metselaar en P.C. Adriaanse, *Grensoverschrijdende inning van bestuurlijke boetes. Een verkennend onderzoek naar ervaringen in België, Duitsland en het Verenigd Koninkrijk en mogelijkheden voor internationale samenwerking*, 10 juni 2014, te raadplegen via: https://www.wodc.nl/onderzoeksdatabase/2305-grensoverschrijdende-inning-van-bestuurlijke-boetes.aspx. Zie hierover eveneens het preadvies van R.E. Tak en R. Klein, Over de grens gaan: grensoverschrijdende handhaving van het mededingings- en consumentenrecht.

4 Rechtsmacht in de praktijk

In de praktijk verwerken momenteel met name grote Amerikaanse spelers zoals Google Inc. en Facebook Inc. grote hoeveelheden persoonsgegevens van Europese burgers. Om deze partijen binnen de reikwijdte van de Privacyrichtlijn te brengen, zien we een tendens om de territoriale reikwijdte van de Privacyrechtlijn, en daarmee de bevoegdheden van de nationale privacytoezichthouders, steeds verder op te rekken. Met name het vestigingsbegrip uit de Privacyrichtlijn is meerdere keren onderwerp geweest van prejudiciële vragen aan het Hof van Justitie EU. Twee van de belangrijkste arresten worden hierna kort besproken. Daarbij wordt tevens aandacht besteed aan de (on)mogelijkheid voor een nationale toezichthouder om sancties op te leggen indien een verantwoordelijke persoonsgegevens van de onderdanen van een lidstaat verwerkt, maar niet aan het nationale recht van die lidstaat onderworpen is, bijvoorbeeld omdat de verantwoordelijke in een andere lidstaat gevestigd is. Daarnaast wordt gekeken naar een actuele zaak waarin rechtsmacht een belangrijke rol speelt, te weten het delen van persoonsgegevens van gebruikers van whatsapp met Facebook Inc. en haar groepsmaatschappijen als gevolg van de overname van WhatsApp Inc. door Facebook Inc.

Tot slot wordt kort stilgestaan bij de rol van de burgerlijke rechter. Het verkrijgen van bestuurlijke rechtsmacht betekent namelijk niet dat hiermee ook de rechtsmacht van de nationale burgerlijke rechter vaststaat. Dit blijkt onder meer uit een kort geding dat is aangespannen door de Belgische privacytoezichthouder tegen Facebook en dat hierna uitgebreider wordt toegelicht.

4.1 Google Spain

De *Google Spain*-zaak[74] is met name bekend vanwege het feit dat het Hof van Justitie EU in deze zaak het 'recht om vergeten te worden' erkent. Maar deze zaak is ook vanuit het oogpunt van het bepalen van het toepasselijke recht zeer interessant. Hier volgen in het kort de feiten op een rij. De heer Costeja González ('Costeja') had eind jaren negentig socialezekerheidsschulden. Nadat beslag werd gelegd op een aantal onroerende zaken, vond er een openbare executoriale veiling plaats. Deze veiling werd meerdere malen in een lokaal dagblad aangekondigd. Op een gegeven moment digitaliseert de krant en is het archief van het dagblad online beschikbaar en daardoor indexeerbaar voor de zoekmachine Google Search. Via Google Search worden wereldwijd websites geïndexeerd, waaronder in Spanje. Google Inc. gebruikt de verzamelde informatie om met zoektermen verbonden advertenties te tonen wanneer iemand Google Search gebruikt. Wanneer iemand de voor- en achternaam van Costeja in de zoekmachine Google invoert, verschijnen er links naar de voornoemde dagbladpublicaties. Costeja wil deze links verwijderd zien, aangezien hij meent dat deze niet meer relevant zijn. Nadat hij bij Google Spain SL en Google Inc. bot vangt, dient hij een klacht in bij de Spaanse toezichthouder, de Agencia Española de Proteccion de Datos ('AEPD'). De AEPD beveelt daarop Google Spain SL en Google Inc. om de gegevens van Costeja uit hun index te verwijderen, zodat in de toekomst niet meer naar de dagbladpublicaties gelinkt wordt. Google Spain SL en Google Inc. stappen vervolgens naar de rechter om het oordeel van de AEPD nietig te laten verklaren. De nationale rechter besluit diverse prejudiciële vragen aan het Hof van Justitie EU te stellen, waarbij ik mij hierna alleen zal richten op de vragen omtrent de materiële en territoriale werkingssfeer van de Privacyrichtlijn.

[74] Zie noot 37.

Voor wat betreft de materiële werkingssfeer van de Privacyrichtlijn, vraagt de rechter zich af of het indexeren van informatie door zoekmachines kan worden aangemerkt als het verwerken van persoonsgegevens en als dat zo is, of de exploitant van een zoekmachine als verantwoordelijke (i.c. Google Inc.) kan worden aangewezen. Deze vragen worden bevestigend beantwoord (zie r.o. 28 e.v.).[75]
Om de territoriale werkingssfeer van de Privacyrichtlijn vast te kunnen stellen, wil de nationale rechter vernemen of Google Spain SL kan worden aangemerkt als 'vestiging' van Google Inc. Dat dit voor de Spaanse rechter niet vanzelfsprekend was, blijkt uit een andere prejudiciële vraag: hij wil weten of het gebruik van *spiders* en robots (computerprogramma's die geautomatiseerd en methodisch het internet doorzoeken) is aan te merken als het gebruik van 'middelen' voor de verwerking van persoonsgegevens (ofwel: geen vestiging maar wel middelen die tot toepassing van het nationale recht kunnen leiden). Hetzelfde wil hij vernemen ten aanzien van het gebruik van een nationale domeinnaam, het sturen van zoekopdrachten en resultaten in de taal van de desbetreffende lidstaat, en de tijdelijke opslag van geïndexeerde informatie. Saillant detail is dat Google Inc. uit concurrentieoverwegingen weigert de plaats aan te geven waar de indexen worden opgeslagen.

Google Spain SL promoot en verkoopt advertentieruimte ten behoeve van Google Search. Zij richt zich hierbij op Spaanse inwoners. Google Spain SL oefent via een vaste vestiging daadwerkelijk economische activiteiten uit (zie r.o. 48). Maar is daarbij sprake van het verwerken van persoonsgegevens in het kader van de activiteiten van een vestiging van Google Inc. in Spanje? Het indexeren van persoonsgegevens voor Google Search wordt gedaan door Google Inc. Google Spain SL verricht alleen reclameactiviteiten. Artikel 4, eerste lid 1, onder a, Privacyrichtlijn eist echter niet dat Google Spain SL *zelf* de gegevensverwerking uitvoert, maar dat de gegevensverwerking plaatsvindt *in het kader van de activiteiten van* Google Spain SL. Het Hof komt tot de conclusie dat de activiteiten van Google Inc. en die van Google Spain SL *onlosmakelijk* met elkaar zijn verbonden: zonder advertenties is de zoekmachine niet economisch rendabel en zonder de zoekmachine hoeven er geen advertenties te worden verkocht (zie r.o. 56). De weergave van de zoekresultaten vormt een gegevensverwerking en op het moment dat de zoekresultaten getoond worden, worden op dezelfde webpagina de daarmee verbonden advertenties getoond. Dit betekent volgens het Hof dat de verwerking wordt verricht in het kader van de reclame- en handelsactiviteiten van Google Spain SL en dat daarmee wordt voldaan aan de eisen van artikel 4, eerste lid, onder a, Privacyrichtlijn. De vragen omtrent het al dan niet aanwezig zijn van middelen voor de verwerking van persoonsgegevens op het grondgebied van een lidstaat van de Europese Unie, in dit specifieke geval Spanje, hoeven derhalve niet meer te worden beantwoord: de toepasselijkheid van de Privacyrichtlijn staat immers vast.

Om te bepalen of een gegevensverwerking plaatsvindt in het kader van de activiteiten van een vestiging van een verantwoordelijke en of aldus het nationale recht van de lidstaat van die vestiging van toepassing is, wordt door het Hof een nieuw element toegevoegd, namelijk de 'onlosmakelijke verbondenheid van activiteiten' ('*inextricably linked'*) van een vestiging van de verantwoordelijke met de gegevensverwerking door de verantwoordelijke zelf. De uitspraak in deze zaak leidde ertoe dat de Artikel 29 Werkgroep zich genoodzaakt zag haar advies inzake het toepasselijk recht aan te passen.[76] Deze uitbreiding van de territoriale reikwijdte van de Privacyrichtlijn kan tot gevolg hebben dat een gegevensverwerking door een

[75] In deze zaak stond niet ter discussie dat geïndexeerde zoekresultaten persoonsgegevens bevatten (zie r.o. 27).
[76] Article 29 Data Protection Working Party, Update of Opinion 8/2010 on applicable law in light of the CJEU Judgement in Google Spain, adopted on 16 December 2015, *WP* 179 (nog niet in het Nederlands beschikbaar).

verantwoordelijke van buiten de EU – die dacht dat hij geen relevante vestigingen voor een bepaalde gegevensverwerking had binnen de EU – toch binnen het toepassingsbereik van de Privacyrichtlijn wordt gebracht.

4.2 Weltimmo

Ook in de zaak *Weltimmo*[77] bleek dat de uitleg van het begrip 'vestiging', ruim twintig jaar na publicatie van de Privacyrichtlijn, nog steeds vragen opriep. Het in Slowakije geregistreerde bedrijf Weltimmo s.r.o. ('Weltimmo') heeft een vastgoedwebsite waarop advertenties kunnen worden geplaatst voor onroerend goed in Hongarije. Advertenties zijn de eerste maand gratis. Een grote groep adverteerders meldt zich na een maand af bij Weltimmo. Weltimmo negeert deze afmeldingen. Als adverteerders weigeren te betalen, stuurt Weltimmo een incassobureau op de adverteerders af. De adverteerders hebben hierover een klacht ingediend bij de Hongaarse privacytoezichthouder, die aan Weltimmo een boete van ongeveer € 32.000 heeft opgelegd. Weltimmo gaat hiertegen in beroep, omdat zij meent dat de Hongaarse toezichthouder geen bevoegdheid toekomt, nu Weltimmo geen vestiging heeft in Hongarije en de server waarop de website gehost wordt, zich niet in Hongarije bevindt.

Uiteindelijk leidt een en ander tot prejudiciële vragen bij het Hof van Justitie EU. De verwijzende rechter vraagt zich allereerst af of het Hongaarse recht van toepassing is op een verantwoordelijke (Weltimmo) die *uitsluitend* in een andere lidstaat is gevestigd (Slowakije), terwijl op de door hem beheerde vastgoedwebsite (ook) advertenties voor in Hongarije gelegen onroerend goed staan, waarbij de persoonsgegevens van de adverteerders vanaf Hongaars grondgebied worden gestuurd naar en worden opgeslagen en bewerkt op een server van de verantwoordelijke (Weltimmo) die weer in een andere lidstaat staat.

Tegelijkertijd wil de rechter weten of bovenstaande feiten ertoe leiden dat artikel 28, eerste lid, Privacyrichtlijn (de aanwijzing van een toezichthouder op het grondgebied van een lidstaat), zo moet worden uitgelegd dat Hongaars recht juist wel of niet kan worden toegepast. Ook wil de rechter vernemen of het voor het bepalen van het toepasselijke nationale recht relevant is dat de website zich op Hongarije richt, de persoonsgegevens vanuit Hongarije zijn ingevoerd op de website, het persoonsgegevens van Hongaarse burgers betreft, en de eigenaren van Weltimmo in Slowakije wonen.

Bij de beantwoording van de vragen maakt het Hof meteen duidelijk dat het de vragen van de verwijzende rechter aldus interpreteert dat het niet duidelijk is of Weltimmo *uitsluitend* in Slowakije is gevestigd. Ook stelt het Hof voorop dat voor de bepaling van het toepasselijke nationale recht artikel 28 Privacyrichtlijn geen rol speelt.

Voor de uitleg van het begrip 'vestiging' verwijst het Hof naar de uitleg die daarin is gegeven in het *Google Spain*-arrest: het begrip 'vestiging' moet ruim worden geïnterpreteerd, maar dat betekent niet dat het enkele feit dat Weltimmo geregistreerd staat in Slowakije, zou betekenen dat zij daar gevestigd is (zie r.o. 28 en 29). Van belang zijn de mate van duurzaamheid van de vestiging in Hongarije en het daadwerkelijke uitoefenen van activiteiten in Hongarije. Hierbij moet ook worden gekeken naar de specifieke aard van de bedrijfsuitoefening en de dienstverlening, in het bijzonder wanneer diensten uitsluitend via het internet

[77] HvJ EU 1 oktober 2015, C-230/14, ECLI:EU:C:2015:639 (*Weltimmo*).

worden aangeboden (zie r.o. 29). Het Hof concludeert dan ook dat, gelet op de doelstellingen van de Privacyrichtlijn (het voorkomen van wetsontduiking en het bieden van een doeltreffende en volledige bescherming van het recht op eerbiediging van de persoonlijke levenssfeer), er onder bepaalde omstandigheden al sprake kan zijn van een duurzame vestiging – zelfs indien er maar één vertegenwoordiger is – indien 'diegene optreedt met een voldoende mate van duurzaamheid en met behulp van de nodige middelen voor de verlening van de betrokken concrete diensten in de desbetreffende lidstaat' (zie r.o. 30). Het begrip 'vestiging' heeft volgens het Hof betrekking op 'iedere vorm van reële en daadwerkelijke activiteit, zelfs geringe, die via een duurzame vestiging wordt uitgeoefend' (r.o. 31).[78]

De exploitatie van de Hongaarse vastgoedwebsites door Weltimmo kan worden aangemerkt als een reële en daadwerkelijke activiteit in Hongarije (r.o. 32). Weltimmo heeft een bankrekening en een brievenbus in Hongarije en een vertegenwoordiger die in Hongarije woonachtig is. De vennootschap bestaat waarschijnlijk maar uit een of twee personen. De vertegenwoordiger treedt op als contactpersoon in bestuurlijke en juridische procedures en treft met klanten betalingsregelingen. Deze elementen tonen aan dat er sprake is van een 'vestiging' (zie r.o. 33). Hetzelfde geldt voor het feit dat de activiteiten hoofdzakelijk op Hongarije zijn gericht (zie r.o. 41, tweede gedachtestreepje).
De verwerking van persoonsgegevens – het plaatsen van persoonsgegevens van adverteerders op internet – door Weltimmo vindt plaats 'in het kader van de activiteiten' van deze vestiging in Hongarije. Hongaars recht is derhalve op deze gegevensverwerking van toepassing (zie r.o. 39). De nationaliteit van de betrokkenen (degenen die de advertenties plaatsen) speelt geen rol bij de bepaling van het nationale recht.

Vervolgens gaat het Hof in op de bevoegdheden van de Hongaarse toezichthouder om op het eigen grondgebied op te treden in de – in deze zaak fictieve – situatie dat niet het Hongaarse maar het Slowaakse recht van toepassing zou zijn. Mag de toezichthouder dan de boetebevoegdheden uitoefenen die hij op grond van het Hongaarse recht heeft?

Het Hof bevestigt dat de Hongaarse toezichthouder op grond van artikel 28, zesde lid, Privacyrichtlijn bevoegd is om, ongeacht welk nationale recht van toepassing is, op zijn eigen grondgebied onderzoek te verrichten, waarbij hij een beroep kan doen op alle bevoegdheden die hem op grond van het *Hongaarse* recht als implementatie van artikel 28, derde lid, Privacyrichtlijn zijn toebedeeld. De Hongaarse toezichthouder kan echter geen sancties opleggen die hem krachtens het Hongaarse recht zijn toegekend, indien het *Slowaakse* recht van toepassing is. Hij zou dan immers zijn nationaalrechtelijke bepalingen toepassen *buiten* zijn grondgebied (zie r.o. 55 e.v.).

Het Hof volgt de Advocaat-Generaal (A-G), die dit punt in zijn conclusie duidelijk uitwerkt.[79] De A-G verwijst allereerst naar overweging 21 van de Privacyrichtlijn, waarin is opgenomen dat de Privacyrichtlijn de territorialiteitsregels inzake het strafrecht onverlet laat (zie r.o. 50 met de verwijzing naar voetnoot 30 bij de conclusie). Hij meent dat dit ook geldt voor administratieve sancties. Het opleggen van een administratieve sanctie door Hongarije zou strijd opleveren met de territoriale soevereiniteit van Slowakije:

[78] Uit het enkele feit dat een website van een bedrijf in een land toegankelijk is en daardoor zijn activiteiten mede op dat land richt, kan niet worden afgeleid dat een bedrijf in dat land een vestiging heeft. Zie HvJ EU 28 juli 2016, C-191/15, ECLI:EU:C:2016:612 (*VfK/Amazon*).
[79] Conclusie A-G P. Cruz Villalón 25 juni 2015, C-230/14, ECLI:EU:C:2015:426 (*Weltimmo*).

staten mogen in beginsel geen publiek gezag uitoefenen buiten hun eigen grondgebied. Ook zou dit strijdig zijn met het legaliteitsbeginsel: het overheidshandelen moet gebaseerd zijn op een vooraf aanwezige wettelijke bepaling. De privacytoezichthouder kan zijn sanctiebevoegdheden niet uitoefenen buiten de wettelijke grenzen waarin hij op grond van zijn nationale recht bevoegd is om op te treden. Hiervan kan alleen worden afgeweken als er een specifieke wettelijke grondslag is die de toepassing van het Hongaarse publiekrecht in Slowakije toestaat en afbakent. Deze bepaling moet voldoende gedetailleerd en duidelijk zijn zodat rechtssubjecten weten dat ze aan dit recht zijn onderworpen en wat de consequenties hiervan kunnen zijn (zie r.o. 50). Oftewel: het moet op voorhand duidelijk zijn dat door een buitenlandse toezichthouder een boete voor bepaald handelen kan worden opgelegd.

Volgens de A-G voldoet de samenwerkingsverplichting zoals neergelegd in artikel 28, zesde lid, Privacyrichtlijn niet aan deze eisen. Er wordt immers niets bepaald over het toepassingsgebied, de werkingssfeer en de waarborgen die nodig zijn voor de toepassing van boetebepalingen van de ene lidstaat in het territoir van de andere lidstaat. De A-G meent dan ook dat in een situatie waarin er een scheiding is tussen het toepasselijke recht en de bevoegde autoriteit, een toezichthouder het opleggen van sancties dient over te laten aan de toezichthouder die op grond van het nationale recht bevoegd is om over de inhoudelijke aspecten van de naleving van de nationale wetgeving te oordelen. [80]

Ter illustratie nogmaals op een rij: Een privacytoezichthouder in land A kan derhalve, als op een gegevensverwerking door een partij het nationale recht van lidstaat B van toepassing is, wel onderzoek verrichten op zijn eigen grondgebied naar mogelijke privacyschendingen door deze partij, maar bij constatering van een dergelijke schending niet de sancties opleggen die hem op grond van het recht van lidstaat A toekomen. Hij kan wel aan de privacytoezichthouder in land B vragen de zaak te onderzoeken en te bezien of er ook in strijd met het nationale recht van land B wordt gehandeld. Als dat het geval is, hangt het ervan af of de nationale wetgeving in land B het toestaat deze schending te sanctioneren. De privacytoezichthouder van land B kan bij zijn eigen onderzoek dan gebruikmaken van de informatie die hij van de privacytoezichthouder in land A heeft ontvangen.

4.3 Facebook en WhatsApp

Facebook Inc. heeft in januari 2014 de chatdienst WhatsApp Inc. overgenomen. Destijds garandeerde zowel Facebook Inc. als WhatsApp Inc. dat zij geen persoonsgegevens van gebruikers zouden gaan uitwisselen. Deze belofte bleek van korte duur: op 25 augustus 2016 kondigde WhatsApp Inc. aan haar gebruikersvoorwaarden en privacybeleid per 25 september 2016 aan te passen. WhatsApp Inc. zou vanaf dat moment accountinformatie van gebruikers gaan delen met Facebook Inc. en haar groepsmaatschappijen (Facebook), onder meer om spam te bestrijden maar vooral ook om relevante aanbiedingen en advertenties te kunnen tonen. Welke data nu wel of niet met Facebook gedeeld zouden worden, is uit het privacybeleid niet af te leiden. Indien gebruikers niet met deze voorwaarden akkoord gingen, konden ze na 25 september 2016 niet meer whatsappen. Nadat een gebruiker akkoord ging met de voorwaarden, had hij dertig dagen de tijd om via de instellingen van zijn smartphone het datadelen met Facebook uit te schakelen. Daarna konden de instellingen niet meer worden aangepast. Een en ander leidde tot veel ophef en de

[80] Zie ook: Article 29 Data Protection Working Party, Advice paper on the practical implementation of the Article 28(6) of the Directive 95/46/EC, Ref. Ares (2011)444105 - 20/04/2011.

privacytoezichthouder van de Duitse deelstaat Hamburg vaardigde op 27 september 2016 een administratief bevel uit, waarin hij Facebook heeft verboden om accountinformatie van Duitse whatsapp-gebruikers te verzamelen en alle informatie die al was verzameld, te vernietigen:

> 'It is clear that Facebook must respect German data protection law after the ECJ confirmed in its ruling from July,[81] that national data protection laws are applicable if a company processes data in connection with a national subsidiary. Facebook is doing this through its subsidiary in Hamburg, which is responsible for the operation of the marketing business in German speaking regions.' [82]

Facebook heeft inmiddels beroep tegen dit bevel ingesteld en stelt zich ook in deze zaak op het standpunt dat de verantwoordelijke voor de gegevensverwerking Facebook Ireland Ltd. is, waardoor zij niet aan Duits maar aan Iers privacyrecht zou zijn onderworpen. Inmiddels is ook de Britse toezichthouder een onderzoek naar zowel Whatsapp Inc. als Facebook Inc. gestart. Dit onderzoek heeft erin geresulteerd dat Facebook Inc. heeft toegezegd om voorlopig geen accountinformatie van Britse whatsapp-gebruikers voor advertentiedoeleinden en productverbetering te gebruiken.[83] In dezelfde periode heeft de Artikel 29 Werkgroep in een open brief aan WhatsApp Inc. ook haar zorgen geuit.[84] Facebook Inc. besloot daarop deze 'pauze' voor de gehele Europese Unie van toepassing te laten zijn en met de Artikel 29 Werkgroep in gesprek te gaan. Het is nu afwachten welke gevolgen een en ander heeft voor mogelijke juridische procedures in de verschillende lidstaten.

4.4 Facebook/Belgische Privacycommissie

Met de uitspraken in *Google Spain* en *Weltimmo* in de hand probeerde de Belgische Privacycommissie Facebook aan te pakken in een *civiele* procedure.[85] Kort samengevat registreerde Facebook door middel van zogenoemde *social plug-ins*[86] en specifieke *cookies* welke websites werden bezocht door Belgische internetgebruikers die geen *Facebook*-account hebben. Hierdoor kon Facebook het individuele surfgedrag van deze personen volgen, waaruit gevoelige informatie kan worden afgeleid. Het feit dat iemand bepaalde webpagina's bezoekt, kan bijvoorbeeld indiceren dat iemand aan een ernstige ziekte lijdt of dat hij een bepaalde seksuele voorkeur heeft. Facebook verkreeg voor het plaatsen van deze *cookies* geen

---

[81] Zie noot 78.

[82] The Hamburg Commissioner for Data Protection and Freedom of Information, Press release: Administrative order against the mass synchronization of data between Facebook and WhatsApp, 27 september 2016, te raadplegen via: https://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/Press_Release_2016-09-27_Adminstrative_Order_Facebook_WhatsApp.pdf.

[83] Information Commissioner's Office, Information Commissioner updates on WhatsApp/Facebook investigation, blogpost 8 november 2016, te raadplegen via: https://iconewsblog.wordpress.com/2016/11/07/information-commissioner-updates-on-whatsapp-facebook-investigation/.

[84] Article 29 Data Protection Working Party, Letter from the Art. 29 WP regarding WhatsApp updated Terms of Service and Privacy Policy, 27 oktober 2016, te raadplegen via: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-ocument/files/2016/20161027__letter_of_the_chair_of_the_art_29_wp_whatsapp_en.pdf.

[85] Rb. Brussel 9 november 2015, nr. 222/2015.

[86] Een *plug-in* is een stukje content dat een website-eigenaar kan inbouwen op zijn webpagina waarmee een functionaliteit van een website van een derde partij wordt aangeboden. Een *social plug-in* is een *plug-in* die verwijst naar social media. Voorbeelden van social plug-ins zijn de 'Vind-ik-leuk'-knop en de knop 'Delen' van Facebook.

geïnformeerde toestemming van de niet-gebruikers van *Facebook*. De Belgische Privacycommissie startte een kort geding tegen Facebook Inc., Facebook Ireland Ltd. en Facebook BVBA om deze flagrante schending van het, volgens haar Belgische, privacyrecht aan te pakken. De privacy van een enorme groep Belgische internetgebruikers wordt immers geschonden, nu miljoenen websites gebruikmaken van *social plug-ins*, waardoor ontsnappen aan de lange arm van Facebook eigenlijk onmogelijk is.

Facebook wordt in de EU – en dus ook in België – aangeboden door de Ierse vennootschap, Facebook Ireland Ltd. Facebook heeft ook een vestiging in België, Facebook Belgium BVBA. Facebook Belgium BVBA is opgericht toen *Facebook* al ruim 4 miljoen leden had in België, om de relaties met de overheid te onderhouden en om te lobbyen. Facebook stelt dat Facebook Ireland Ltd. als de verantwoordelijke voor de gegevensverwerking moet worden aangemerkt. Derhalve is volgens Facebook het Ierse en niet het Belgische privacyrecht van toepassing en kan alleen de Ierse privacytoezichthouder optreden. Daarnaast komt de Belgische civiele rechter volgens Facebook ten aanzien van deze zaak geen rechtsmacht toe om zich over deze zaak uit te laten.

De Belgische Privacycommissie stelt zich op het standpunt dat het Belgische privacyrecht van toepassing is en dat de Belgische rechter bevoegd is. De rechtbank volgt dit standpunt. Het doet er volgens haar niet toe of nu Facebook Inc. of Facebook Ireland de verantwoordelijke is voor de gegevensverwerking. Facebook Ireland Ltd. maakt deel uit van het Facebook-concern. Facebook Belgium BVBA is een vestiging van de verantwoordelijke in België. De hoofdactiviteit van Facebook Belgium BVBA is het bieden van ondersteuning aan het publieke beleid, de verkoop en de levering van marketingdiensten ten behoeve van het Facebook-concern. Volgens de Belgische Privacycommissie betekent dit dat de *activiteiten* van Facebook Belgium BVBA, in lijn met de uitspraak van het Hof van Justitie EU in de *Google Spain*-zaak, onlosmakelijk verbonden zijn met de *activiteiten* van de voor de gegevensverwerking verantwoordelijke. De gegevensverwerking hoeft immers niet '*door*' Facebook Belgium BVBA te worden verricht, maar slechts '*in het kader van de activiteiten*' van deze vestiging. Het verzamelen van de informatie over het surfgedrag vindt volgens de Privacycommissie plaats in het kader van de reclame-en handelsactiviteiten van Facebook Belgium BVBA. Ook het lobbywerk en het onderhouden van relaties met de overheid zijn activiteiten die Facebook rendabel moeten maken en zijn daarom onlosmakelijk met de verantwoordelijke verbonden (zie par. 3.1 van de uitspraak). Nu het gaat over het toepassen van Belgische wetgeving op Belgisch grondgebied en Facebook Belgium BVBA een vestiging van de voor de gegevensverwerking verantwoordelijke is, zou de Belgische rechter (civiele (!)) rechtsmacht bezitten. De rechtbank besluit dan ook Facebook Inc., Facebook Ireland Ltd. en Facebook Belgium BVBA te gelasten om binnen 48 uur na betekening van haar beschikking op last van een dwangsom van € 250.000 per dag te stoppen met het plaatsen van de *cookies* bij niet-gebruikers van *Facebook*, alsmede het uitlezen daarvan via *social plug-ins* op websites van derden.

In hoger beroep oordeelt het Hof anders.[87] Facebook betwist dat de Belgische rechter civiele rechtsmacht toekomt ten aanzien van Facebook Ireland Ltd. en Facebook Inc. Voordat het toepasselijke privacyrecht wordt vastgesteld, dient eerst een oordeel geveld te worden over de civiele rechtsmacht van de Belgische rechter. Volgens de Belgische Privacycommissie heeft de Belgische rechter rechtsmacht, op grond van artikel 28 Privacyrichtlijn, waarin – zoals eerder uiteengezet – is opgenomen dat iedere lidstaat een

[87] Hof Brussel 29 juni 2016, nr. 5747/2016.

toezichthouder kan aanwijzen die belast is met het toezicht op de toepassing van de Privacyrichtlijn op het grondgebied van de desbetreffende lidstaat (zie r.o. 15 e.v.). In België is dit de Belgische Privacycommissie, die op grond van artikel 32, derde paragraaf van de Belgische Wet Verwerking Persoonsgegevens (WVP)[88] bevoegd is om ieder geschil aangaande de toepassing van WVP aan de rechter voor te leggen. Daarmee wordt echter geen civiele rechtsmacht over Facebook Ireland Ltd. en Facebook Inc. gecreëerd, aldus het Hof. Het beroep op *Google Spain* en *Weltimmo* helpt de Privacycommissie niet. In Google Spain waren Google Spain SL en Google Inc. zelf de eisende partijen, die door het starten van een procedure bij de Spaanse rechtbank de civiele rechtsmacht van de Spaanse rechter hadden aanvaard, aldus het Hof. In *Weltimmo* wordt geen uitspraak gedaan over de *civiele* rechtsmacht, maar wordt de vraag beantwoord of de Hongaarse toezichthouder bevoegdheid had om op te treden. Het Slowaakse *Weltimmo* had zelf een vordering bij de Hongaarse rechtbank ingesteld en daarmee de civiele rechtsmacht van de Hongaarse rechter aanvaard. Dat in *Weltimmo* wordt gesteld dat de toezichthoudende autoriteiten hun bevoegdheden moeten uitoefenen in overeenstemming met het procedurele recht van hun eigen lidstaten (zie r.o. 50 *Weltimmo*), betekent niet dat de Belgische rechter rechtsmacht heeft over alle geschillen in België. Dat zou volgens het Hof een onjuiste lezing zijn van de reikwijdte van het arrest (zie r.o. 25). Een beroep op artikel 4, eerste lid, onder a, Privacyrichtlijn biedt evenmin soelaas: dat artikel heeft enkel betrekking op de bepaling van het toepasselijke privacyrecht. De Privacyrichtlijn heeft niet ten doel een harmonisatie tot stand te brengen ten aanzien van de civiele rechtsmacht of de bevoegdheid van de rechters van de lidstaten (zie r.o. 28). Een beroep op het ontlenen van civiele rechtsmacht aan de Brussel Ibis-Verordening[89] slaagt evenmin, omdat het een geschil tussen een vennootschap en overheid betreft, waarbij de overheid handelt in de uitoefening van haar overheidstaak, hetgeen buiten het materiële toepassingsbereik van de Verordening valt (zie r.o. 39 en 40). De Belgische Privacycommissie zal daarom moeten aantonen dat de Belgische rechter bevoegdheid toekomt op grond van de Belgische wet (zie r.o. 32-35 en r.o. 44-46). Omdat Facebook Belgium BVBA in België gevestigd is, is de Belgische rechter op grond van haar nationale wetgeving bevoegd om kennis te nemen van tegen deze entiteit ingestelde vorderingen. Dat geldt echter niet voor Facebook Inc. en Facebook Ireland Ltd.

Hoewel de Belgische rechter zich derhalve bevoegd achtte om kennis te nemen van de tegen Facebook Belgium BVBA ingestelde vordering, schiet de Belgische Privacycommissie daar uiteindelijk weinig mee op. Omdat het een kortgedingprocedure betreft, moet 'hoogdringendheid' (vergelijkbaar met het naar Nederlands recht geldende vereiste dat sprake moet zijn van 'spoedeisend belang') van de vorderingen worden aangetoond door de Belgische Privacycommissie. Facebook plaatst deze *cookies* al sinds 2011. Nu deze schending al sinds jaar en dag geschiedt, wordt aan de eis van hoogdringendheid niet voldaan (zie r.o. 57-59). Zo staat de Belgische Privacycommissie uiteindelijk met lege handen.

[88] Wet van 8 december 1992 voor de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *B.S.* 18 maart 1993.

[89] Verordening (EU) Nr. 1215/2012 van het Europees Parlement en de Raad van 12 december 2012 betreffende de rechterlijke bevoegdheid, de erkenning en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken, (*PbEU* 2012, L351/1).

5 De nabije toekomst: rechtsmacht onder de Europese Privacyverordening

5.1 Materiële en territoriale werkingssfeer

5.1.1 Algemeen

De implementatie van de Privacyrichtlijn binnen de Europese Unie heeft niet geleid tot volledige harmonisatie van het privacyrecht in de lidstaten. Met name op het gebied van sanctieoplegging bestaan grote verschillen. Ook wordt middels kunstgrepen (er is *wel* een vestiging, maar *geen* relevante vestiging, maar *wel* middelen, dus *toch* rechtsmacht ...) nationaal recht van toepassing verklaard. Een en ander komt de rechtszekerheid en de rechtsbescherming niet ten goede. Ook kan dit leiden tot een belemmering van het vrije verkeer van persoonsgegevens en kan dit de mededinging verstoren (zie overweging 9 Privacyverordening). De Europese wetgever heeft er daarom voor gekozen de Privacyrichtlijn te vervangen door een Privacyverordening. Nu een verordening rechtstreekse werking heeft, en derhalve niet hoeft te worden omgezet in nationale wetgeving, kan de privacywetgeving in de Europese Unie op een coherente manier worden toegepast. Dit moet rechtszekerheid bieden en maakt het mogelijk om consistent toezicht uit te oefenen. Hierbij dient wel te worden opgemerkt dat de lidstaten eerst hun huidige wetgeving dienen 'op te ruimen', hetgeen heel wat voeten in de aarde kan hebben. Sommige wetgeving zal niet meer relevant zijn en komen te vervallen, andere wetgeving dient te worden aangepast op de Privacyverordening, en op bepaalde gebieden staat het lidstaten vrij om nadere regels vast te stellen, zoals bij gegevensverwerking in het kader van arbeidsverhoudingen. Dit betekent derhalve dat volledige harmonisatie van de privacywetgeving in de EU niet zal worden bereikt. In Nederland wordt momenteel gewerkt aan een specifieke uitvoeringswet voor de Privacyverordening, die de Wbp zal gaan vervangen.

5.1.2 Materiële werkingssfeer

De materiële werkingssfeer van de Privacyverordening is niet wezenlijk anders dan die van de Privacyrichtlijn, zie artikel 2 Privacyverordening. Wat opvalt, is dat nadrukkelijk wordt benoemd dat voor de instellingen, organen en instanties van de Europese Unie, Verordening 45/2001 blijft gelden. Op dit punt vindt evenmin harmonisatie plaats. Wel zal Verordening 45/2001 waar nodig worden aangepast (zie overweging 17 Privacyverordening). Verder is van belang om op te merken dat de definitie van het begrip 'persoonsgegeven' aanzienlijk is uitgebreid, zie artikel 4, eerste lid, Privacyverordening. Hoewel uit de jurisprudentie al bleek dat dit begrip ruim dient te worden geïnterpreteerd, is nu onder meer expliciet opgenomen dat *online identifiers*, zoals *cookies* en IP-adressen, als persoonsgegevens kunnen kwalificeren. Daarnaast legt de Privacyverordening niet alleen verplichtingen op aan de verantwoordelijke, maar ook direct aan de verwerker (zie bijv. art. 28 en 33, tweede lid, Privacyverordening).[90]

[90] In de Wbp was het begrip 'verwerker' uit de Privacyrichtlijn geïmplementeerd als '***be***werker'. In de Nederlandse vertaling van de Privacyverordening wordt wederom gesproken over de 'verwerker'.

5.1.3 Territoriale werkingssfeer

Vestiging van een verantwoordelijke of verwerker in de Europese Unie

De territoriale werkingssfeer is aanzienlijk gewijzigd en we zien verschillende elementen uit de Europese jurisprudentie terugkomen. De Privacyverordening is allereerst van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of verwerker (eigen onderstreping) in de Europese Unie, *ongeacht of de verwerking al dan niet in de Unie plaatsvindt* (eigen cursivering) (art. 3, eerste lid, Privacyverordening). De toevoeging van de verwerker in deze bepaling roept meteen een vraag op. Betekent dit dat als een verantwoordelijke die buiten de Europese Unie is gevestigd, een Europese verwerker inschakelt, daardoor de Privacyverordening indirect ook op de verantwoordelijke van toepassing wordt voor de specifieke gegevensverwerking die hij door de verwerker laat verrichten? Dat zou de commerciële positie van Europese verwerkers niet ten goede komen. Maar gelet op de huidige Privacyrichtlijn, waarin het gebruik van middelen in de Europese Unie tot toepasselijkheid van het recht van één van de lidstaten kan leiden, zou een dergelijke uitleg niet bevreemdend zijn. Dit zou echter kunnen betekenen dat de Privacyverordening op gegevensverwerkingen die nauwelijks of zelfs geen band hebben met de Europese Unie, van toepassing zou kunnen zijn. De Artikel 29 Werkgroep noemde dit eerder een ongewenst bijeffect in het kader van het bepalen van de territoriale werkingssfeer in het licht van de Privacyrichtlijn.[91] Zolang deze bepaling niet nader wordt toegelicht of uitgelegd, lijkt dit risico onder de Privacyverordening ook te bestaan.

Aanbieden van goederen of diensten of monitoren van gedrag

De Privacyverordening is eveneens van toepassing op de verwerking van persoonsgegevens van betrokkenen die zich in de Unie bevinden, door een niet in de Europese Unie gevestigde verantwoordelijke of verwerker, wanneer de verwerking verband houdt met: (a) het aanbieden van goederen of diensten aan deze betrokkenen in de Europese Unie, ongeacht of een betaling door de betrokkenen is vereist, en (b) het monitoren van hun gedrag, voor zover dit gedrag in de Europese Unie plaatsvindt (art. 3, tweede lid, Privacyverordening). In dat geval dient de verantwoordelijke of de verwerker schriftelijk een vertegenwoordiger aan te wijzen (art. 27, eerste lid, Privacyverordening). Er gelden uitzonderingen voor incidentele verwerkingen van persoonsgegevens waarbij er een laag risico is voor de rechten en vrijheden van de betrokkenen, alsmede voor overheidsinstanties en -organen (zie art. 27, tweede lid, Privacyverordening). De vertegenwoordiger moet gevestigd zijn in één van de lidstaten waar de betrokkenen waarvan persoonsgegevens worden verwerkt (om hen te monitoren of aan hen producten of diensten aan te bieden) zich bevinden (zie art. 27, derde lid, Privacyverordening).
Voordeel van deze bepaling is dat de discussie over en het oprekken van de notie ‘middelen voor de gegevensverwerking in de Europese Unie’ tot het verleden behoort. Indien er wel een vestiging is, maar die is niet bij de gegevensverwerking betrokken, dan hoeft niet meer te worden bepaald of deze vestiging als irrelevant kan worden aangemerkt en er alsnog toepasselijkheid van het Europese privacyrecht via het aanwezig zijn van ‘middelen’ in de lidstaten kan worden geconstrueerd.

[91] Zie noot 64.

Als we kijken naar het eerder besproken voorbeeld van Whatsapp Inc. (zie par. 3.1), dan volstaat onder de Privacyverordening dat wordt aangetoond dat Whatsapp Inc. een dienst aanbiedt aan betrokkenen in de Europese Unie. Hetzelfde geldt voor de toepasselijkheid van Europees privacyrecht op Google Inc., Facebook Inc. e.d. Er zijn geen ingewikkelde constructies meer nodig om de activiteiten van de ene vestiging onlosmakelijk verbonden te laten zijn met de gegevensverwerking door de verantwoordelijke; voortaan kan 'simpelweg' de vraag worden beantwoord of een partij persoonsgegevens in het kader van het aanbieden van zijn goederen of diensten aan betrokkenen in de Europese Unie verwerkt. In de overwegingen bij de Privacyverordening wordt hierover opgemerkt dat bepaald moet worden of een verantwoordelijke of verwerker '*klaarblijkelijk voornemens'* is om diensten of goederen aan te bieden aan betrokkenen in een of meer lidstaten van de Europese Unie. Het gegeven dat een website, e-mailadres of andere contactgegevens in de Europese Unie toegankelijk zijn, is onvoldoende om dit aan te nemen. Ook het feit dat een website bijvoorbeeld in het Engels is opgesteld, is niet doorslaggevend. Aanknopingspunten voor toepasselijkheid van de Privacyverordening kunnen worden gevonden in het gegeven dat er andere talen van de lidstaten worden gebruikt en producten of diensten ook in die taal kunnen worden besteld, dat het mogelijk is om in euro's of andere Europese valuta te betalen of dat een website melding maakt van Europese klanten (zie overweging 23 Privacyverordening). Dit zijn elementen die we kennen uit het consumentenrecht. Ik verwacht dat de uitleg van deze bepaling in de praktijk weer tot een stroom van jurisprudentie zal leiden, want wat moet worden verstaan onder 'klaarblijkelijk voornemens'? Kan dit objectief worden uitgelegd? En wellicht is een partij helemaal niet van plan om zich te richten op de Europese Unie, maar heeft zijn Engelstalige website, waar met een creditcard betaald kan worden voor een online dienst, wel veel Europese klanten. Moet hij dan, om onder de reikwijdte van de Privacyverordening uit te komen, via technische middelen zijn website ontoegankelijk maken voor betrokkenen in de Europese Unie?

Het element 'ongeacht of de betrokkenen hiervoor moeten betalen' is van belang omdat juist bij gratis diensten vaak geen geldelijke betaling, maar een betaling in persoonsgegevens plaatsvindt. Sommige diensten kunnen bijvoorbeeld alleen maar gratis zijn doordat zij gepersonaliseerde advertenties aan de betrokkene aanbieden, waarvoor het surfgedrag en/of andere gedragingen van de betrokkene moeten worden gevolgd.

De notie 'monitoren van gedrag van betrokkenen in de Europese Unie' verdient enige toelichting. Het gaat erom of een verantwoordelijke of verwerker iemands gedrag binnen de Europese Unie controleert, bijvoorbeeld door hem met behulp van *tracking cookies* of andere technieken te volgen op het internet (zie overweging 24 Privacyverordening). Om te kunnen vaststellen of er sprake is van controle, dient ook te worden gekeken of daarbij een profiel wordt opgesteld van de betrokkenen waardoor de persoonlijke voorkeuren en het gedrag van de betrokkenen kunnen worden geanalyseerd of voorspeld, of waardoor er bepaalde besluiten over hem genomen kunnen worden (bijvoorbeeld of hij bepaalde aanbiedingen wel of niet te zien krijgt of voor een product meer of minder betaalt dan een ander).

Een andere gedachte die achter de brede territoriale reikwijdte schuilt, is niet zozeer het beschermen van de privacy, maar het creëren van eerlijke concurrentie in een geglobaliseerde wereld via een gelijk *level*

playing field tussen Europese en niet-Europese partijen.[92] Nu is het immers zo dat partijen die in Europa gevestigd zijn, aan het Europese privacyrecht onderworpen zijn, terwijl er niet-Europese partijen bestaan die zonder de beperkingen die de Europese wetgeving aan hun dienstverlening stelt, persoonsgegevens van Europese burgers kunnen verwerken en vercommercialiseren. Deze doelstelling is in de literatuur bekritiseerd. Zo merkt Svantesson op dat de Privacyverordening dusdanig zware lasten en verplichtingen voor het midden- en kleinbedrijf met zich brengt, dat het de vraag is of het toetreden tot de Europese markt niet alleen is voorbehouden aan grote multinationals die het zich kunnen veroorloven om zich aan de Europese wetgeving te houden en aan bedrijven die überhaupt niet van plan zijn om de wetgeving na te leven.[93]

De bepaling aangaande de toepasselijkheid van de Privacyverordening op grond van de plaats waar een verantwoordelijke krachtens het internationale publiekrecht gevestigd is, is ongewijzigd ten opzichte van de Privacyrichtlijn (art. 3, derde lid, Privacyverordening).

5.2 Toezicht

Op grond van artikel 51 Privacyverordening moeten de lidstaten een onafhankelijke toezichthouder aanwijzen. Deze toezichthouder heeft rechtsmacht op het grondgebied van zijn lidstaat, in de zin dat hij de taken en bevoegdheden (zie art. 57 en 58 Privacyverordening) die hij op grond van de Privacyverordening heeft, in zijn lidstaat kan uitvoeren en uitoefenen (zie art. 55, eerste lid, Privacyverordening). Voor de AP betekent dit dat wanneer een gegevensverwerking plaatsvindt in het kader van activiteiten van een vestiging van een verantwoordelijke of een verwerker in Nederland, zij in beginsel rechtsmacht heeft. Ook komt de AP rechtsmacht toe wanneer een verantwoordelijke of een verwerker niet in de EU gevestigd is, maar persoonsgegevens verwerkt omdat er goederen of diensten worden aangeboden aan betrokkenen in Nederland of wanneer hun gedrag wordt gemonitord, voor zover dit gedrag in Nederland plaatsvindt.

Alle toezichthouders hebben door de Privacyverordening dezelfde onderzoeks- en handhavingsbevoegdheden, waaronder het opleggen van substantiële boetes (zie art. 83 Privacyverordening). Wel dienen deze bevoegdheden conform het lidstatelijke procesrecht te worden uitgevoerd.

Ook onder de nieuwe Privacyverordening zullen zich vele situaties kunnen voordoen waarin verantwoordelijken en verwerkers in verschillende lidstaten van de Europese Unie gevestigd zijn, goederen en diensten worden aangeboden in verschillende lidstaten en/of gedrag van betrokkenen in bepaalde lidstaten of zelfs de gehele Europese Unie wordt gemonitord. Welke toezichthouders zijn dan bevoegd om op te treden?

Onder de nieuwe Privacyverordening kunnen meerdere toezichthouders tegelijkertijd bevoegd zijn wanneer er sprake is van een *grensoverschrijdende* verwerking. Volgens artikel 4, onder 24, Privacyverordening is

[92] Zie speech van Eurocommisaris Reding, 'The EU Data Protection Regulation: Promoting Technological Innovation and Safeguarding Citizen's Rights, Brussel 4 maart 2014, te raadplegen via: http://europa.eu/rapid/press-release_SPEECH-14-175_en.htm.

[93] D.J.B. Svantesson, 'Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the Regulation', *International Data Privacy Law* 2015, Vol. 5, nr. 4, p. 230.

hiervan allereerst sprake indien een gegevensverwerking plaatsvindt in het kader van de activiteiten van meerdere vestigingen van een verantwoordelijke of een verwerker in de Europese Unie. Een voorbeeld hiervan is een centrale HR-database voor de Europese entiteiten van een verantwoordelijke of verwerker, waarbij de gegevens in één centraal datacenter worden opgeslagen. Er kan ook sprake zijn van grensoverschrijdende gegevensverwerkingen wanneer betrokkenen in meerdere lidstaten wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden van een gegevensverwerking die in het kader van de activiteiten van één vestiging van een verantwoordelijke of een verwerker plaatsvindt. Een voorbeeld hiervan is de huidige werkwijze van Facebook Inc. waarbij vanuit Facebook Ireland Ltd. de Europese Unie bediend wordt. De notie 'wezenlijke gevolgen' is niet nader in de Privacyverordening uitgewerkt.

In dergelijke gevallen treedt een soort *land-van-oorsprongstelsel* in werking. De autoriteit van het land waar de verantwoordelijke of de verwerker zijn hoofdvestiging of enige vestiging heeft (art. 56, eerste lid, Privacyverordening), treedt op als leidende toezichthoudende autoriteit. In overweging 36 van de Privacyverordening is een en ander nader uitgewerkt. De hoofdvestiging van een verantwoordelijke is de plaats van zijn centrale administratie, tenzij het doel en de middelen van de gegevensverwerking door een andere vestiging in de Europese Unie worden bepaald, zie artikel 4, onder 16, onder a, Privacyverordening. In dat geval wordt deze vestiging als hoofdvestiging aangewezen. Voor de bepaling van de hoofdvestiging is niet van belang of de persoonsgegevens al dan niet op de locatie van de hoofdvestiging worden verwerkt. Voor een verwerker geldt eveneens de plaats van de centrale administratie als leidraad voor het bepalen van de hoofdvestiging, zie artikel 4, onder 16, onder b, Privacyverordening. Indien een centrale administratie ontbreekt, geldt als hoofdvestiging de plaats waar de voornaamste verwerkingsactiviteiten in de Europese Unie plaatsvinden. Indien zowel een verantwoordelijke als een verwerker bij een gegevensverwerking betrokken is, is de toezichthoudende autoriteit van de lidstaat waar de verantwoordelijke zijn hoofdvestiging heeft, de leidende toezichthoudende autoriteit. Bij een gegevensverwerking door een concern geldt dat de hoofdvestiging van de zeggenschap uitoefenende onderneming als de hoofdvestiging van het concern wordt beschouwd, tenzij het doel van en de middelen voor de verwerking door een andere onderneming worden bepaald.

Wat betekent dit voor de rechtsmacht van de AP? Kan zij nog optreden tegen privacyschendingen bij grensoverschrijdende verwerkingen waarbij zij niet als leidende toezichthoudende autoriteit wordt aangemerkt? In de Privacyverordening is voor dergelijke gevallen voorzien in een samenwerkingsprocedure. De leidende toezichthoudende autoriteit moet samenwerken met de andere bevoegde toezichthouders, de zogenaamde 'betrokken toezichthoudende autoriteiten'. De wijze van samenwerking is gedetailleerd uitgewerkt in de artikelen 60 tot en met 62 Privacyverordening. Zo zijn toezichthouders onder meer verplicht relevante informatie uit te wisselen en elkaar wederzijdse bijstand te verlenen. Ook kunnen zij gezamenlijk onderzoek uitvoeren, onder bepaalde voorwaarden ook op elkaars grondgebied (art. 62, derde lid, Privacyverordening). De leidende toezichthoudende autoriteit dient haar ontwerpbesluit eerst voor te leggen aan de andere toezichthouders en rekening te houden met hun standpunten. Doel is het bereiken van consensus. Ook is er een procedure opgetuigd om geschillen tussen toezichthouders te beslechten (zie art. 65 Privacyverordening). Tevens bestaat er een spoedprocedure die het mogelijk maakt dat toezichthouders, ook als zij niet als de leidende toezichthoudende autoriteit kwalificeren, op het eigen grondgebied kortstondig maatregelen kunnen nemen om de privacy van de betrokkenen op hun grondgebied te beschermen (zie art. 66 Privacyverordening).

Daarnaast behoudt de AP haar rechtsmacht bij gegevensverwerkingen die plaatsvinden op grond van een nationale wettelijke verplichting of ter uitvoering van een nationale publiekrechtelijke taak (zie art. 55, tweede lid, Privacyverordening). Ook mag de AP, in afwijking van de hoofdregel, een bij haar ingediende klacht of een inbreuk op de Privacyverordening behandelen indien het onderwerp van de zaak alleen verband houdt met een vestiging van een verantwoordelijke of verwerker in Nederland of alleen in Nederland wezenlijke gevolgen heeft (zie art. 56, tweede lid, Privacyverordening). Zoals reeds is opgemerkt, blijft de AP bevoegd om op het Nederlandse grondgebied de taken uit te voeren en de bevoegdheden uit te oefenen die de Privacyverordening haar toekent (art. 55 Privacyverordening).

Voor verantwoordelijken en verwerkers heeft het nieuwe systeem het voordeel dat zij bij grensoverschrijdende gegevensverwerkingen met één toezichthouder te maken hebben: een *one-stop-shop* (zie art. 56, zesde lid, Privacyverordening). Het voordeel voor betrokkenen is dat zij bij elke toezichthoudende autoriteit een klacht mogen indienen, indien de betrokkene meent dat een verwerking inbreuk maakt op de Privacyverordening (zie art. 77, eerste lid, Privacyverordening). De eerder door de AP geuite zorgen dat een *land-van-oorsprongstelsel* het voor de betrokkene moeilijker zou maken om zijn recht te halen, lijken hiermee te zijn weggenomen.[94]

Wat ik echter mis in de Privacyverordening, is een competentiebepaling voor die gevallen waarin een verantwoordelijke of verwerker *niet* in de Europese Unie gevestigd is, maar op grond van artikel 3, tweede lid, Privacyverordening *wel* binnen de territoriale reikwijdte van de Privacyverordening valt. Vaak zullen goederen of diensten worden aangeboden (en vindt er een daaraan gerelateerde gegevensverwerking plaats) in meerdere lidstaten en zal derhalve sprake zijn van grensoverschrijdende verwerkingen. Ook het online volgen van betrokkenen zal veelal niet beperkt zijn tot een lidstaat. Hoe wordt dan bepaald welke toezichthouder de leidende toezichthoudende autoriteit is? Dient dan te worden aangehaakt bij het land waar de vertegenwoordiger van de verantwoordelijke of de verwerker gevestigd is? Artikel 27, derde lid, Privacyverordening geeft niet aan in welke lidstaat een vertegenwoordiger gevestigd moet zijn. Kan dit wellicht tot gevolg hebben dat partijen een vertegenwoordiger aanwijzen in een land waar men weet dat de handhavingscapaciteit van de nationale toezichthouder beperkt is en derhalve het risico om aangesproken te worden op niet-naleving van de bepalingen van de Privacyverordening minder aannemelijk lijkt? Of kan in dit geval geen beroep worden gedaan op de *one-stop-shop* en moet in dergelijke gevallen met verschillende toezichthouders rekening worden gehouden? Verduidelijking van de criteria is wenselijk, niet alleen om te voorkomen dat de rechtsbescherming van de betrokkenen wordt aangetast, maar ook om ervoor te zorgen dat niet-Europese verantwoordelijken en verwerkers weten aan wie zij verantwoording verschuldigd zijn.

[94] Zie noot 30, p. 289.

6 Conclusies en stellingen

U heeft het volgehouden om dit preadvies uit te lezen, chapeau! Want als er één ding duidelijk is geworden, is het wel dat de bepaling van de rechtsmacht van de toezichthouders, zowel onder de huidige Europese Privacyrichtlijn, als onder de nieuwe Privacyverordening, een bijzonder complex onderwerp is. Via kunstgrepen is in de Europese jurisprudentie de territoriale reikwijdte van de Europese Privacyrichtlijn steeds verder uitgebreid. Het komt de rechtszekerheid ten goede dat deze uitbreidingen in gemeenschapsrecht zijn omgezet door codificering in de nieuwe Privacyverordening. Of de Privacyverordening echt een einde maakt aan de rechtsonzekerheid, waag ik echter te betwijfelen. Ook de nieuwe bepalingen roepen namelijk tal van vragen op. Daarnaast is het de vraag of de Privacyverordening adequaat gehandhaafd kan worden wanneer de betrokken partijen gevestigd zijn buiten de Europese Unie. Hierbij speelt eveneens het gegeven dat er geen internationale afspraken zijn over de grensoverschrijdende inning van bestuurlijke boetes, hetgeen de daadwerkelijke rechtsmacht van de privacytoezichthouders ondermijnt.

Voor bedrijven en betrokkenen is het bijzonder prettig dat zij vaak nog maar met één toezichthouder te maken hebben. Wel dient het voor bedrijven die niet in de Europese Unie gevestigd zijn, maar waarop de Privacyverordening wel van toepassing is, duidelijk te zijn welke toezichthouder(s) dat is/zijn. Hier ligt dan ook een taak voor de Artikel 29 Werkgroep om een en ander uit te werken, zodat definitieve richtsnoeren hierover door haar opvolger, het Europees Comité voor gegevensbescherming, kunnen worden aangenomen.

Voor toezichthouders betekent de nieuwe Privacyverordening dat zij hun rechtsmacht bij grensoverschrijdende gegevensverwerkingen moeten delen met andere toezichthouders en daarbij niet altijd *in charge* zullen zijn. De AP krijgt een duidelijke set bevoegdheden binnen het Nederlandse grondgebied. Zij zal in bepaalde gevallen als leidende toezichthoudende autoriteit of, in het kader van gezamenlijke onderzoeken, als één van de toezichthouders deze bevoegdheden kunnen uitoefenen in samenwerking met andere toezichthouders. Maar het hebben van rechtsmacht betekent mijns inziens ook dat je daar als toezichthouder gebruik van dient te maken. Voorkomen moet worden dat onduidelijkheden over de interpretatie van de rechtsmacht van de nationale toezichthouders kunnen leiden tot lacunes in de rechtsbescherming, zoals in Nederland in het verleden het geval is geweest. Zowel onder de huidige als onder de toekomstige regelgeving geldt daarom voor de AP dat grenzeloos zeker niet machteloos maakt, maar de AP deze macht wel moet grijpen. Ik ben mij er daarbij terdege van bewust dat budgettaire beperkingen hierbij eveneens een rol kunnen spelen.

Om tot een afronding te komen poneer ik de volgende stellingen:

1. De gewenste extraterriotoriale werking en de daarmee gepaard gaande privacybescherming van Europese burgers die de Privacyverordening nastreeft, kan alleen worden bereikt indien het Europees Comité voor gegevensbescherming de voorwaarden voor de toepasselijkheid van de Privacyverordening op gegevensverwerkingen door een niet in de Europese Unie gevestigde verantwoordelijke of verwerker, nader specificeert.

2. Zolang er geen internationale afspraken worden gemaakt over het invorderen van bestuurlijke boetes, biedt de rechtsmacht die door de extraterritoriale werking van de Privacyverordening wordt gecreëerd, geen effectieve rechtsbescherming.