HOF VAN JUSTITIE
VAN DE EUROPESE UNIE
DIRECTIE ONDERZOEK
EN DOCUMENTATIE

Themafiche

BESCHERMING VAN PERSOONSGEGEVENS

Het recht op bescherming van persoonsgegevens is een grondrecht en de eerbiediging ervan vormt een belangrijk doel voor de Europese Unie.

Het is verankerd in het Handvest van de grondrechten van de Europese Unie (hierna: „Handvest"), dat in artikel 8 bepaalt:

„1. Eenieder heeft recht op bescherming van zijn persoonsgegevens.

2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht van inzage in de over hem verzamelde gegevens en op rectificatie daarvan.

3. Een onafhankelijke autoriteit ziet erop toe dat deze regels worden nageleefd."

Dit grondrecht houdt voorts nauw verband met het recht op eerbiediging van het privéleven en van het familie- en gezinsleven, dat is vervat in artikel 7 van het Handvest.

Het recht op bescherming van persoonsgegevens is tevens vastgelegd in artikel 16, lid 1, van het Verdrag betreffende de werking van de Europese Unie (VWEU), dat daartoe in de plaats is gekomen van artikel 286 EG.

Wat het afgeleide recht betreft, heeft de Europese Gemeenschap zich vanaf midden jaren negentig verschillende instrumenten verschaft waarmee de bescherming van persoonsgegevens moest worden verzekerd. Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens[1], die is vastgesteld op grondslag van artikel 100 A EG, vormde in dit opzicht de belangrijkste Uniehandeling op dat gebied. Hierin waren de algemene voorwaarden voor rechtmatigheid van de verwerking van deze gegevens alsmede de rechten van de betrokkenen vastgelegd en was met name bepaald dat in de lidstaten onafhankelijke toezichthoudende autoriteiten werden ingesteld.

[1] 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 (PB 1995, L 281, blz. 31), geconsolideerde versie van 20 november 2003, ingetrokken per 25 mei 2018 (zie voetnoot 5).

Richtlijn 2002/58/EG[2] bracht vervolgens een aanvulling op richtlijn 95/46, met een harmonisering van de regelgeving van de lidstaten inzake de bescherming van de persoonlijke levenssfeer, met name bij de verwerking van persoonsgegevens in de sector elektronische communicatie.[3] Opgemerkt moet worden dat de Uniewetgever voornemens is deze richtlijn opnieuw te bezien. In dit verband heeft de Commissie op 10 januari 2017 een voorstel ingediend ter vervanging van die richtlijn door een verordening betreffende privacy en elektronische communicatie.[4]

Binnen de ruimte van vrijheid, veiligheid en recht (oud artikelen 30 en 31 VEU) regelde voorts, tot mei 2018, kaderbesluit 2008/977/JBZ[5] de bescherming van persoonsgegevens op het gebied van politiële en justitiële samenwerking in strafzaken.

In 2016 heeft de Europese Unie het algemene rechtskader op dit gebied herzien. Daartoe heeft de Unie verordening (EU) 2016/679[6] betreffende gegevensbescherming (hierna: „AVG") vastgesteld, waarbij richtlijn 95/46 is ingetrokken en die toepasselijk is sinds 25 mei 2018, alsmede richtlijn (EU) 2016/680[7] inzake bescherming van die gegevens in strafzaken, waarbij kaderbesluit 2008/977/JBZ is ingetrokken en waarin 6 mei 2018 is vastgelegd als termijn voor omzetting door de lidstaten.

Ten slotte was in het kader van de verwerking ervan door de instellingen en organen van de EU de bescherming van persoonsgegevens eerst verzekerd door verordening (EG) nr. 45/2001[8]. Op basis van deze verordening kon in 2004 de Europese Toezichthouder voor gegevensbescherming in het leven worden geroepen. In 2018 werd de Unie uitgerust met een nieuw rechtskader hiervoor, met name door de vaststelling van verordening (EU) 2018/1725[9], waarbij verordening nr. 45/2001 en besluit nr. 1247/2002/EG[10] zijn ingetrokken en die van toepassing is sinds 11 december 2018. In het belang van een coherente benadering van de

---

2 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB 2002, L 201, blz. 37), geconsolideerde versie van 19 december 2009.

3 Richtlijn 2002/58 is gewijzigd bij richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van richtlijn 2002/58/EG (PB 2006, L 105, blz. 54). Deze richtlijn is door het Hof in het arrest van 8 april 2014, Digital Rights Ireland en Seitlinger e.a. (C-293/12 en C-594/12, EU:C:2014:238), ongeldig verklaard omdat zij een ernstige aantasting vormde van het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens (zie rubriek I.1, met het opschrift **„**Overeenstemming van het afgeleide Unierecht met het recht op bescherming van persoonsgegevens**"** van deze fiche).

4 Voorstel voor een verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie) COM/2017/010 final – 2017/03 (COD).

5 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 (PB 2008, L 350, blz. 60), ingetrokken per 6 mei 2018 (zie voetnoot 7).

6 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/EG (PB 2016, L 119, blz. 1).

7 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 (PB 2016, L 119, blz. 89).

8 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 persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens (PB 2001, L 8, blz. 1).

9 Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van verordening (EG) nr. 45/2001 en besluit nr. 1247/2002/EG.

10 Besluit nr. 1247/2002/EG van het Europees Parlement, de Raad en de Commissie van 1 juli 2002 betreffende het statuut en de algemene voorwaarden voor de uitoefening van het ambt van Europees toezichthouder voor gegevensbescherming (PB 2002, L 183, blz. 1).

bescherming van persoonsgegevens in de gehele Unie, beoogt deze nieuwe verordening de desbetreffende voorschriften zoveel mogelijk aan te passen aan het bij de AVG gecreëerde stelsel.

INHOUD

I. In het Handvest van de grondrechten van de Europese Unie erkend recht op bescherming van persoonsgegevens

1. Overeenstemming van het afgeleide Unierecht met het recht op bescherming van persoonsgegevens

Arrest van 9 november 2010 (Grote kamer), Volker und Markus Schecke en Eifert (C-92/09 en C-93/09, EU:C:2010:662)[11]

In deze zaak stonden in de hoofdgedingen landbouwers en het Land Hessen tegenover elkaar met betrekking tot de bekendmaking, op de website van de Bundesanstalt für Landwirtschaft und Ernährung (Duits federaal instituut voor landbouw en voedselvoorziening), van persoonsgegevens die hen betroffen in hun hoedanigheid van begunstigden van financiële middelen uit het Europees Landbouwgarantiefonds (ELGF) en het Europees Landbouwfonds voor plattelandsontwikkeling (Elfpo). Die landbouwers verzetten zich tegen die bekendmaking met het argument, in het bijzonder, dat die bekendmaking niet was gerechtvaardigd door een zwaarder wegend openbaar belang. Het Land Hessen meende dat de bekendmaking van die gegevens voortvloeide de verordeningen (EG) nr. 1290/2005[12] en nr. 259/2008[13], die de regeling inzake de financiering van het gemeenschappelijk landbouwbeleid bevatten en bekendmaking van informatie over de natuurlijke personen die begunstigden zijn van het ELGF en het Elfpo, verplicht stellen.

In deze context heeft het Verwaltungsgericht Wiesbaden (bestuursrechter Wiesbaden, Duitsland) het Hof verschillende vragen voorgelegd over de geldigheid van een aantal bepalingen van verordening nr. 1290/2005 en van verordening nr. 259/2008, op grond waarvan dergelijke informatie ter beschikking van het publiek moet worden gesteld, met name middels websites van de nationale instanties.

Het Hof heeft met betrekking tot het op elkaar afstemmen van het in het Handvest erkende recht op bescherming van persoonsgegevens en de transparantieverplichting op het gebied van Europese fondsen opgemerkt dat de bekendmaking op een website van de nominatieve gegevens betreffende de begunstigden van de fondsen en de door hen ontvangen bedragen, wegens de vrije toegang van derden tot de website een aantasting vormt van het recht van de

[11] Dit arrest is opgenomen in het Jaarverslag 2010, blz. 11.

[12] Verordening (EG) nr. 1290/2005 van de Raad van 21 juni 2005 betreffende de financiering van het gemeenschappelijk landbouwbeleid (PB 2005, L 209, blz. 1), ingetrokken bij verordening (EU) nr. 1306/2013 van het Europees Parlement en de Raad van 17 december 2013 inzake de financiering, het beheer en de monitoring van het gemeenschappelijk landbouwbeleid (PB 2013, L 347, blz. 549).

[13] Verordening (EG) nr. 259/2008 van de Commissie van 18 maart 2008 tot vaststelling van uitvoeringsbepalingen van verordening (EG) nr. 1290/2005 van de Raad met betrekking tot de bekendmaking van informatie over de begunstigden van financiële middelen uit het ELGF en het Elfpo (PB 2008, L 76, blz. 28), ingetrokken bij uitvoeringsverordening (EU) nr. 908/2014 van de Commissie van 6 augustus 2014 houdende uitvoeringsbepalingen van verordening (EU) nr. 1306/2013 van het Europees Parlement en de Raad, wat betreft betaalorganen en andere instanties, financieel beheer, goedkeuring van de rekeningen, voorschriften inzake controles, zekerheden en transparantie (PB 2014, L 255, blz. 59).

betrokken begunstigden op eerbiediging van hun privéleven in het algemeen en op de bescherming van hun persoonsgegevens in het bijzonder (punten 56-64).

Om gerechtvaardigd te zijn, moet een dergelijke aantasting bij wet zijn voorzien, de wezenlijke inhoud van die rechten eerbiedigen en, met inachtneming van het evenredigheidsbeginsel, noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang, en moeten de afwijkingen en beperkingen op die rechten binnen de grenzen van het strikt noodzakelijke blijven (punt 65). In deze context heeft het Hof geoordeeld dat de belastingplichtigen in een democratische samenleving weliswaar het recht hebben om te worden geïnformeerd over het gebruik van overheidsmiddelen, doch dat dit niet wegneemt dat de Raad en de Commissie een evenwichtige afweging van de verschillende betrokken belangen dienden te maken, waarvoor, vóór de vaststelling van de betwiste bepalingen, moest worden nagegaan of de bekendmaking van die gegevens middels één website per lidstaat, niet verder ging dan noodzakelijk was voor de verwezenlijking van de nagestreefde rechtmatige doelstellingen (punten 77, 79, 85 en 86).

Het Hof heeft dus bepaalde voorschriften van verordening nr. 1290/2005 alsmede verordening nr. 259/2008 in haar geheel ongeldig verklaard voor zover deze bepalingen ten aanzien van natuurlijke personen die steun uit het ELGF en het Elfpo hebben ontvangen, voorzien in de verplichte bekendmaking van persoonsgegevens betreffende iedere begunstigde, zonder dat daarbij onderscheid wordt gemaakt op basis van relevante criteria, zoals de tijdvakken waarin zij die steun hebben ontvangen, de frequentie, het type en de omvang van de steunverlening (punt 92 en dictum 1). Volgens het Hof wordt evenwel niet teruggekomen op de gevolgen van de bekendmaking van de lijsten van begunstigden van dergelijke steun waartoe de nationale autoriteiten tijdens de periode vóór de datum van het arrest waren overgegaan (punt 94 en dictum 2).

Arrest van 17 oktober 2013, Schwarz (C-291/12, EU:C:2013:670)

Schwarz verzocht bij de gemeente Bochum (Duitsland) om afgifte van een paspoort, waarbij hij echter weigerde zijn vingerafdrukken te laten afnemen. Aangezien de gemeente zijn verzoek afwees, stelde Schwarz beroep in bij het Verwaltungsgericht Gelsenkirchen (bestuursrechter Gelsenkirchen, Duitsland) waarbij hij vorderde dat deze gemeente werd bevolen hem een paspoort af te geven zonder afname van zijn vingerafdrukken. Voor deze rechter betwistte Schwarz de geldigheid van verordening (EG) nr. 2252/2004[14], waarbij de verplichting is ingevoerd om van de aanvragers van paspoorten vingerafdrukken af te nemen. Hij betoogde daartoe onder meer dat deze verordening het recht op bescherming van persoonsgegevens en het recht op eerbiediging van het privéleven schendt.

In deze context heeft het Verwaltungsgericht Gelsenkirchen zich tot het Hof gewend met een verzoek om een prejudiciële beslissing teneinde te vernemen of die verordening, voor zover daarbij de aanvrager van een paspoort wordt verplicht zijn vingerafdrukken te laten nemen en er wordt voorzien in opname daarvan in het paspoort, geldig is, met name in het licht van het Handvest.

[14] Verordening (EG) nr. 2252/2004 van de Raad van 13 december 2004 betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten (PB 2004, L 385, blz. 1), zoals gewijzigd bij verordening (EG) nr. 444/2009 van het Europees Parlement en de Raad van 6 mei 2009 (PB 2009, L 142, blz. 1).

Het Hof heeft bevestigend geantwoord, door te oordelen dat het afnemen van vingerafdrukken en de opname daarvan in het paspoort door de nationale autoriteiten, zoals geregeld door artikel 1, lid 2, van verordening nr. 2252/2004, weliswaar een aantasting van de rechten op eerbiediging van het privéleven en bescherming van persoonsgegevens vormen, doch dat deze aantasting gerechtvaardigd is door de doelstelling van bescherming van paspoorten tegen elk frauduleus gebruik.

Om te beginnen wordt met een dergelijke bij wet gestelde beperking een door de Unie erkende doelstelling van algemeen belang nagestreefd, aangezien daarmee met name wordt beoogd te voorkomen dat personen illegaal het grondgebied van de Unie binnenkomen (punten 35-38). Vervolgens zijn het afnemen en het bewaren van de vingerafdrukken geschikt om die doelstelling te verwezenlijken. Hoewel, ten eerste, de methode om de identiteit te verifiëren door middel van vingerafdrukken niet volledig betrouwbaar is, vermindert zij immers aanzienlijk het risico van acceptaties van niet-geautoriseerde personen. Ten tweede betekent het feit dat er geen overeenstemming bestaat tussen de vingerafdrukken van de paspoorthouder enerzijds, en de in dit document aangebrachte gegevens anderzijds, niet dat de betrokkene de binnenkomst op het grondgebied van de Unie automatisch wordt geweigerd, maar heeft dit enkel tot gevolg dat die persoon aan een grondig onderzoek zal worden onderworpen teneinde definitief zijn identiteit te kunnen vaststellen (punten 42-45).

Wat ten slotte de noodzaak van een dergelijke verwerking betreft, is het Hof niet in kennis gesteld van het bestaan van maatregelen die voldoende doeltreffend zijn maar die een minder ingrijpende aantasting meebrengen van de in de artikelen 7 en 8 van het Handvest erkende rechten dan de maatregelen die de op vingerafdrukken gebaseerde methode meebrengt (punt 53). Artikel 1, lid 2, van verordening nr. 2252/2004 brengt geen verwerkingen van vingerafdrukken met zich mee die verder gaan dan voor de verwezenlijking van die doelstelling noodzakelijk is. Die verordening preciseert immers uitdrukkelijk dat vingerafdrukken alleen mogen worden gebruikt voor het verifiëren van de authenticiteit van het paspoort en de identiteit van de houder ervan. Bovendien biedt artikel 1, lid 2, van die verordening bescherming tegen het risico dat gegevens die vingerafdrukken bevatten, worden gelezen door personen die daarvoor geen toestemming hebben, en bepaalt dat artikel dat vingerafdrukken enkel mogen worden bewaard in het paspoort zelf, dat het exclusieve bezit van de houder ervan blijft (punten 54-57, 60 en 63).

Arrest van 8 april 2014 (Grote kamer), Digital Rights Ireland en Seitlinger e.a. (gevoegde zaken C-293/12 en C-594/12, EU:C:2014:238)[15]

Dit arrest is voortgekomen uit verzoeken tot toetsing van de geldigheid van richtlijn 2006/24/EG betreffende het bewaren van gegevens, in het licht van de grondrechten op eerbiediging van het privéleven en op bescherming van persoonsgegevens, welke verzoeken waren ingediend in het kader van nationale gedingen bij de Ierse en de Oostenrijkse gerechten. In zaak C-293/12 was bij de High Court (rechter in eerste aanleg, Ierland) een geding aanhangig gemaakt tussen Digital Rights Ireland en de Ierse autoriteiten over de rechtmatigheid van nationale maatregelen inzake het bewaren van gegevens betreffende elektronische communicatie. In zaak C-594/12 waren bij het Verfassungsgerichtshof (constitutioneel hof, Oostenrijk) verschillende constitutionele

[15] Dit arrest is opgenomen in het Jaarverslag 2014, blz. 60.

beroepen ingesteld waarin nietigverklaring werd gevorderd van de nationale bepaling waarbij richtlijn 2006/24 in Oostenrijks recht was omgezet.

Met hun verzoeken om een prejudiciële beslissing vroegen de Ierse en de Oostenrijkse rechterlijke instantie het Hof of richtlijn 2006/24 geldig was in het licht van de artikelen 7, 8 en 11 van het Handvest. Meer in het bijzonder vroegen zij het Hof of de krachtens die richtlijn op de aanbieders van openbare elektronische-communicatiediensten of van een openbaar communicatienetwerk rustende verplichting om gegevens betreffende het privéleven van een persoon en zijn communicatie, gedurende een bepaalde tijd te bewaren en toegang daartoe toe te staan aan de bevoegde nationale autoriteiten, een ongerechtvaardigde inmenging in die grondrechten impliceerde. De typen gegevens waar het om gaat zijn met name gegevens die nodig zijn om de bron van een communicatie en de bestemming ervan te traceren en te identificeren, om de datum, het tijdstip en de duur van een communicatie alsmede het type communicatie te bepalen, om de communicatieapparatuur van de gebruikers te identificeren alsmede om de locatie van mobiele communicatieapparatuur te bepalen, tot welke gegevens onder meer behoren naam en adres van de abonnee of de geregistreerde gebruiker, het oproepende en het opgeroepen nummer en een IP-adres voor internetdiensten. Aan de hand van deze gegevens kan met name worden nagegaan met welke persoon en via welke weg een abonnee of geregistreerde gebruiker heeft gecommuniceerd, hoelang de communicatie heeft geduurd en vanaf welke plaats zij heeft plaatsgevonden. Bovendien kan aan de hand van deze gegevens worden achterhaald hoe vaak de abonnee of de geregistreerde gebruiker gedurende een bepaalde periode met bepaalde personen heeft gecommuniceerd.

Het Hof heeft om te beginnen geoordeeld dat, door dergelijke verplichtingen op te leggen aan die aanbieders, de bepalingen van richtlijn 2006/24 een bijzonder zware inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten op eerbiediging van het privéleven en op bescherming van persoonsgegevens vormden. In deze context heeft het Hof vastgesteld dat deze inmenging kon worden gerechtvaardigd door een doel van algemeen belang, zoals het bestrijden van georganiseerde misdaad. Daartoe heeft het Hof er in de eerste plaats op gewezen dat het bij de richtlijn opgelegde bewaren van gegevens geen afbreuk deed aan de wezenlijke inhoud van de grondrechten op eerbiediging van het privéleven en op bescherming van persoonsgegevens, voor zover die richtlijn niet de mogelijkheid biedt om kennis te nemen van de inhoud zelf van de elektronische communicaties en bepaalt dat de aanbieders van diensten of van een netwerk bepaalde beginselen van gegevensbescherming en -beveiliging moeten respecteren. In de tweede plaats heeft het Hof opgemerkt dat het bewaren van gegevens met het oog op de eventuele overdracht ervan aan de bevoegde nationale autoriteiten inderdaad beantwoordde aan een doelstelling van algemeen belang, te weten de bestrijding van ernstige criminaliteit, en uiteindelijk de openbare veiligheid (punten 38-44).

Het Hof heeft echter geoordeeld dat de Uniewetgever, door de richtlijn betreffende het bewaren van gegevens vast te stellen, de door het evenredigheidsbeginsel gestelde grenzen had overschreden. Bijgevolg heeft het de richtlijn ongeldig verklaard met de overweging dat de zeer ruime en bijzonder zware inmenging in de grondrechten die zij impliceerde, niet toereikend was gereguleerd teneinde te garanderen dat deze inmenging beperkt was tot het strikt noodzakelijke (punt 65). Richtlijn 2006/24 bestreek immers algemeen elke persoon en alle elektronische-communicatiemiddelen en alle verkeersgegevens, zonder dat enig onderscheid werd gemaakt, enige beperking werd gesteld of enige uitzondering werd gemaakt op basis van het doel, zware criminaliteit te bestrijden (punten 57-59). De richtlijn bevatte ook geen

objectieve criteria ter waarborging dat de bevoegde nationale autoriteiten enkel toegang tot de gegevens hadden en deze enkel konden gebruiken met het oog op het voorkomen, opsporen of strafrechtelijk vervolgen van inbreuken die voldoende ernstig kunnen worden beschouwd om een dergelijke inmenging te rechtvaardigen. Evenmin bevatte zij de materiële en procedurele voorwaarden voor een dergelijke toegang en een dergelijk gebruik (punten 60-62). Wat ten slotte de vraag betreft hoelang de gegevens moesten worden bewaard, bepaalde de richtlijn dat zij zes maanden moesten worden bewaard zonder dat enig onderscheid werd gemaakt tussen de categorieën gegevens op basis van de betrokken personen of het eventuele nut van de gegevens ten opzichte van het nagestreefde doel (punten 63 en 64).

Bovendien heeft het Hof met betrekking tot de uit artikel 8, lid 3, van het Handvest voortvloeiende vereisten vastgesteld dat richtlijn 2006/24 niet voldoende garanties bood om een doeltreffende bescherming van de gegevens te verzekeren tegen het risico van misbruik en tegen onrechtmatige raadpleging en onrechtmatig gebruik van deze gegevens, en evenmin voorschreef dat de betrokken gegevens op het grondgebied van de Unie moesten worden bewaard.

Bijgevolg garandeerde deze richtlijn niet ten volle dat een onafhankelijke autoriteit toezicht houdt op de eerbiediging van de vereisten inzake bescherming en beveiliging, zoals het Handvest evenwel uitdrukkelijk voorschrijft (punten 66-68).

2. Eerbiediging van het recht op bescherming van persoonsgegevens bij de uitvoering van het Unierecht

Arrest van 21 december 2016 (Grote kamer), Tele2 Sverige (gevoegde zaken C-203/15 en C-698/15, EU:C:2016:970)[16]

Nadat het arrest Digital Rights Ireland en Seitlinger e.a. richtlijn 2006/24 ongeldig had verklaard (zie hierboven), zijn bij het Hof twee zaken aanhangig gemaakt over de in Zweden en in het Verenigd Koninkrijk aan aanbieders van elektronische-communicatiediensten opgelegde algemene verplichting om de gegevens betreffende die communicatie te bewaren, hetgeen was voorgeschreven bij de ongeldig verklaarde richtlijn.

De dag na de uitspraak van het arrest Digital Rights Ireland en Seitlinger e.a. heeft het telecommunicatiebedrijf Tele2 Sverige de Zweedse toezichthoudende autoriteit voor post en telecommunicatie ervan in kennis gesteld dat zij de gegevens niet meer zou bewaren en voornemens was de reeds opgeslagen gegevens te wissen (zaak C-203/15). Het Zweedse recht verplichtte immers de aanbieders van elektronische-communicatiediensten om met betrekking tot alle elektronische-communicatiemiddelen stelselmatig en voortdurend, zonder enige uitzondering, alle verkeersgegevens en locatiegegevens van alle abonnees en geregistreerde gebruikers te bewaren. In zaak C-698/15 hadden drie personen beroep ingesteld tegen het Britse stelsel van gegevensbewaring op grond waarvan de minister van Binnenlandse Zaken de openbare telecommunicatiebedrijven kon verplichten alle communicatiegegevens maximaal twaalf maanden te bewaren, waarbij het bewaren van de inhoud van een communicatie echter niet was toegestaan.

[16] Dit arrest is opgenomen in het Jaarverslag 2016, blz. 63.

De Kammarrätt i Stockholm (bestuursrechter in tweede aanleg Stockholm, Zweden) en de Court of Appeal (England and Wales) (Civil Division) (rechter in tweede aanleg in burgerlijke zaken, Engeland en Wales, Verenigd Koninkrijk) wendden zich tot het Hof, dat zich diende uit te spreken over de uitlegging van artikel 15, lid 1, van richtlijn 2002/58, de zogeheten „richtlijn betreffende privacy en elektronische communicatie", op grond waarvan de lidstaten bepaalde uitzonderingen mogen maken op de in die richtlijn geformuleerde verplichting om de vertrouwelijkheid van de communicatie en van de daarmee verband houdende verkeersgegevens te waarborgen.

In zijn arrest heeft het Hof om te beginnen geoordeeld dat artikel 15, lid 1, van richtlijn 2002/58, gelezen tegen de achtergrond van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, zich verzet tegen een nationale regeling zoals die van Zweden, die, ter bestrijding van criminaliteit, voorziet in algemene en ongedifferentieerde bewaring van alle verkeersgegevens en locatiegegevens van alle abonnees en geregistreerde gebruikers betreffende alle elektronische-communicatiemiddelen. Volgens het Hof gaat een dergelijke regeling verder dan strikt noodzakelijk is, en kan zij niet worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals genoemd artikel 15, lid 1, gelezen tegen de achtergrond van voornoemde artikelen van het Handvest, vereist (punten 99-105, 107, 112 en dictum 1).

Diezelfde bepaling, gelezen tegen de achtergrond van dezelfde artikelen van het Handvest, verzet zich tevens tegen een nationale regeling die de bescherming en de beveiliging van de verkeersgegevens en de locatiegegevens en in het bijzonder de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens regelt zonder, in het kader van de bestrijding van criminaliteit, te bepalen dat die toegang alleen wordt verleend ter bestrijding van ernstige criminaliteit, dat die toegang aan een voorafgaand toezicht door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit is onderworpen, en dat de betrokken gegevens op het grondgebied van de Unie moeten worden bewaard (punten 118-122, 125 en dictum 2).

Het Hof heeft overwogen dat artikel 15, lid 1, van richtlijn 2002/58 zich daarentegen niet verzet tegen een regeling op grond waarvan dergelijke gegevens ter bestrijding van zware criminaliteit preventief gericht kunnen worden bewaard, op voorwaarde dat die bewaring, wat de categorieën van betrokken gegevens, de betrokken communicatiemiddelen, de betrokken personen en de duur van de bewaring betreft, tot het strikt noodzakelijke wordt beperkt. Om aan deze eisen te voldoen, moet deze nationale regeling in de eerste plaats duidelijke en nauwkeurige regels bevatten, zodat persoonsgegevens doeltreffend kunnen worden beschermd tegen het risico van misbruik. Zij moet in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een maatregel van bewaring van gegevens preventief kan worden genomen, en aldus waarborgen dat een dergelijke maatregel tot het strikt noodzakelijke wordt beperkt. In de tweede plaats moet – wat de materiële voorwaarden betreft waaraan de nationale regeling moet voldoen om te waarborgen dat zij tot het strikt noodzakelijke is beperkt – de bewaring van de gegevens steeds voldoen aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel. In het bijzonder moeten dergelijke voorwaarden in de praktijk van dien aard blijken te zijn dat zij de omvang van de maatregel, en dus de kring van betrokken personen, daadwerkelijk afbakenen. Wat deze afbakening betreft, moet de nationale regeling worden gebaseerd op objectieve elementen waarmee kan worden gedoeld op een groep mensen wier gegevens, althans indirect, een band met handelingen van zware criminaliteit aan het licht kunnen brengen, waarmee op de een of andere wijze kan

worden bijgedragen tot de bestrijding van zware criminaliteit of waarmee een ernstig risico voor de openbare veiligheid kan worden voorkomen (punten 108-11).

II. Verwerking van persoonsgegevens in de zin van de algemene regeling op dit gebied

1. Verwerking van persoonsgegevens die buiten de werkingssfeer van richtlijn 95/46 valt

Arrest van 30 mei 2006 (Grote kamer), Parlement/Raad (C-317/04 en C-318/04, EU:C:2006:346)

Na de terroristische aanslagen van 11 september 2001 hebben de Verenigde Staten in november van dat jaar een wettelijke regeling vastgesteld volgens welke luchtvaartmaatschappijen die verbindingen naar, vanuit of over het grondgebied van de Verenigde Staten verzorgen, de Amerikaanse autoriteiten elektronische toegang moesten verlenen tot de gegevens in hun boekings- en vertrekcontrolesystemen, Passenger Name Records (PNR) geheten.

Daar zij van mening was dat deze bepalingen in strijd zouden kunnen zijn met de Europese wetgeving en met de wetgeving van de lidstaten inzake gegevensbescherming, heeft de Commissie onderhandelingen gevoerd met de Amerikaanse autoriteiten. Na deze onderhandelingen heeft de Commissie op 14 mei 2004 beschikking 2004/535/EG[17] vastgesteld waarbij werd geconstateerd dat het United States Bureau of Customs and Border Protection (bureau voor douane en grensbescherming van de Verenigde Staten; hierna: „CBP") waarborgen voor een passend beschermingsniveau biedt voor PNR-gegevens die vanuit de Gemeenschap worden doorgegeven (hierna: „gelijkwaardigheidsbeschikking"). Vervolgens heeft de Raad op 17 mei 2004 besluit 2004/496/EG[18] vastgesteld houdende goedkeuring van het sluiten van een overeenkomst tussen de Europese Gemeenschap en de Verenigde Staten inzake de verwerking en overdracht van PNR-gegevens aan het CBP door op het grondgebied van de lidstaten van de Gemeenschap gevestigde luchtvaartmaatschappijen.

Het Europees Parlement heeft het Hof verzocht de twee bovengenoemde handelingen nietig te verklaren met name met het betoog dat de gelijkwaardigheidsbeschikking ultra vires was vastgesteld, dat artikel 95 EG (thans artikel 114 VWEU) niet de juiste rechtsgrondslag was voor het besluit houdende goedkeuring van het sluiten van de overeenkomst en, in beide zaken, dat er sprake was van schending van grondrechten.

[17] Beschikking 2004/535/EG van de Commissie van 14 mei 2004 betreffende de passende bescherming van persoonsgegevens in het Passenger Name Record van vliegtuigpassagiers die aan het Bureau of Customs and Border Protection van de Verenigde Staten worden doorgegeven (PB 2004, L 235, blz. 11).

[18] Besluit 2004/496/EG van de Raad van 17 mei 2004 betreffende de sluiting van een overeenkomst tussen de Europese Gemeenschap en de Verenigde Staten van Amerika inzake de verwerking en overdracht van PNR-gegevens door luchtvaartmaatschappijen aan het Bureau of Customs and Border Protection van het ministerie van Binnenlandse Veiligheid van de Verenigde Staten van Amerika (PB 2004, L 183, blz. 83, met rectificatie in PB 2005, L 255, blz. 168).

Wat de gelijkwaardigheidsbeschikking betreft, heeft het Hof om te beginnen onderzocht of de Commissie haar beschikking rechtsgeldig op grondslag van richtlijn 95/46 kon vaststellen. In deze context stelde het Hof vast dat uit de gelijkwaardigheidsbeschikking bleek dat de doorgifte van de PNR-gegevens aan het CBP een verwerking is die betrekking heeft op de openbare veiligheid en de activiteiten van de staat op strafrechtelijk gebied. Volgens het Hof werden de PNR-gegevens weliswaar aanvankelijk door luchtvaartmaatschappijen verzameld in het kader van een onder het Unierecht vallende activiteit, namelijk de verkoop van een vliegticket dat recht gaf op een dienstverlening, maar was de in de gelijkwaardigheidsbeschikking bedoelde gegevensverwerking van geheel andere aard. Deze beschikking zag namelijk niet op een verwerking die noodzakelijk is voor een dienstverrichting, maar op gegevensverwerking die noodzakelijk werd geacht voor het waarborgen van de openbare veiligheid en voor de wetshandhaving (punten 56 en 57).

In dit verband heeft het Hof opgemerkt dat het feit dat de PNR-gegevens door particuliere marktdeelnemers voor commerciële doeleinden waren verzameld en dat het deze laatste waren die ze doorgaven naar een derde land, er niet aan in de weg stond dat deze doorgifte werd beschouwd als een van de werkingssfeer van de richtlijn uitgesloten gegevensverwerking. Deze doorgifte geschiedde immers binnen een door de overheid ingesteld kader dat betrekking had op de openbare veiligheid. Bijgevolg kwam het Hof tot de slotsom dat de gelijkwaardigheidsbeschikking niet binnen de werkingssfeer van de richtlijn viel, omdat zij een verwerking van persoonsgegevens betrof die daarvan was uitgesloten. Het Hof heeft de gelijkwaardigheidsbeschikking derhalve nietig verklaard (punten 58 en 59).

Wat het besluit van de Raad betreft, stelde het Hof vast dat artikel 95 EG juncto artikel 25 van richtlijn 95/46 niet de grondslag kan vormen voor de bevoegdheid van de Gemeenschap om de betrokken overeenkomst met de Verenigde Staten te sluiten. Die overeenkomst betrof namelijk dezelfde doorgifte van gegevens als de gelijkwaardigheidsbeschikking en dus gegevensverwerkingen die buiten de werkingssfeer van de richtlijn vielen. Bijgevolg heeft het Hof het besluit van de Raad houdende goedkeuring van de sluiting van de overeenkomst nietig verklaard (punten 67-69).

Arrest van 11 december 2014, Ryneš (C-212/13, EU:C:2014:2428)

Nadat hij verschillende keren was lastiggevallen, had Ryneš als reactie daarop aan zijn huis een bewakingscamera gemonteerd. Na een nieuw incident bij zijn huis, konden aan de hand van de opnames van die camera twee verdachten worden geïdentificeerd, jegens wie strafzaken werden ingeleid. Daar de rechtmatigheid van de verwerking van de door de bewakingscamera opgenomen gegevens door een van de verdachten werd betwist bij de Tsjechische instantie voor de bescherming van persoonsgegevens, heeft die instantie vastgesteld dat Ryneš de regels betreffende de bescherming van persoonsgegevens had geschonden en hem een geldboete opgelegd.

Nadat door Ryneš een hogere voorziening was ingesteld tegen een beslissing van de Městský soud v Praze (rechtbank van de stad Praag, Tsjechië), waarbij het besluit van genoemde instantie was bevestigd, heeft de Nejvyšší správní soud (hoogste bestuursrechter) het Hof de vraag voorgelegd of de door Ryneš ter bescherming van zijn leven, gezondheid en eigendom gemaakte opnames een gegevensverwerking vormden die niet onder richtlijn 95/46 viel, omdat

deze opnames door een natuurlijke persoon in activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden waren gemaakt, in de zin van artikel 3, lid 2, tweede streepje, van die richtlijn.

Het Hof heeft geoordeeld dat het gebruik van een camerasysteem dat door een natuurlijke persoon aan zijn gezinswoning werd bevestigd met als doel de eigendom, de veiligheid en het leven van de eigenaren van het huis te beschermen, maar dat ook de openbare ruimte in beeld brengt, en waarbij video-opnames van personen met behulp van opnameapparatuur doorlopend worden vastgelegd op bijvoorbeeld een harde schijf, niet wordt aangemerkt als de verwerking van persoonsgegevens die in activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden wordt verricht in de zin van die bepaling (punt 35 en dictum).

In dit verband heeft het Hof in herinnering gebracht dat de bescherming van het grondrecht op eerbiediging van het privéleven, zoals gewaarborgd in artikel 7 van het Handvest, vereist dat de uitzonderingen op de bescherming van persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven. Aangezien de bepalingen van richtlijn 95/46, die voor de verwerking van persoonsgegevens een regeling vaststelt die afbreuk kan doen aan de fundamentele vrijheden, en in het bijzonder aan het recht op een privéleven, noodzakelijkerwijs moeten worden uitgelegd in het licht van de grondrechten die in het Handvest zijn opgenomen, dient de uitzondering die is voorzien in artikel 3, lid 2, tweede streepje, van die richtlijn, strikt te worden uitgelegd (punten 27-29). Bovendien wordt de verwerking van persoonsgegevens die in activiteiten met „uitsluitend" persoonlijke of huishoudelijke doeleinden wordt verricht, door de bewoordingen zelf van die bepaling aan de werkingssfeer van richtlijn 95/46 onttrokken. Voor zover het gebruik van een videobewakingssysteem – zelfs slechts gedeeltelijk – de openbare ruimte bestrijkt en hierdoor buiten de privésfeer geraakt van degene die door middel van dit systeem gegevens verwerkt, kan het niet worden beschouwd als een activiteit die met uitsluitend „persoonlijke of huishoudelijke doeleinden" wordt verricht in de zin van die bepaling (punten 30, 31 en 33).

2. Begrip „persoonsgegevens"

Arrest van 19 oktober 2016, Breyer (C-582/14, EU:C:2016:779)[19]

Breyer had bij de Duitse civiele rechterlijke instanties beroep ingesteld dat ertoe strekte dat aan de Bondsrepubliek Duitsland een verbod werd opgelegd om de IT-gegevens die na elk bezoek van de websites van de Duitse federale instellingen werden doorgegeven, te bewaren of door derden te doen bewaren. Teneinde cyberaanvallen af te weren en strafvervolging van de aanvallers mogelijk te maken, werden immers door de aanbieder van onlinemediadiensten van de Duitse federale instellingen de gegevens geregistreerd die bestaan in een „dynamisch" IP-adres – een IP-adres dat bij elke nieuwe verbinding met het internet wijzigt –, alsmede de datum en het uur waarop de website werd bezocht. Anders dan bij „statische" IP-adressen, maken dynamische IP-adressen het a priori niet mogelijk om aan de hand van bestanden die voor het publiek toegankelijk zijn, een verband te leggen tussen een bepaalde computer en de fysieke aansluiting op het door de internetprovider gebruikte netwerk. De geregistreerde gegevens boden op zichzelf de aanbieder van onlinemediadiensten niet de mogelijkheid om de gebruiker

[19] Dit arrest is opgenomen in het Jaarverslag 2016, blz. 62.

te identificeren. Daarentegen beschikte de internetprovider zijnerzijds over extra informatie die het mogelijk maakt, wanneer zij wordt gecombineerd met dat IP-adres, die gebruiker te identificeren.

In deze context heeft het Bundesgerichtshof (hoogste federale rechter, Duitsland), waarbij beroep in *Revision* was ingesteld, het Hof gevraagd of een IP-adres dat een aanbieder van onlinemediadiensten opslaat wanneer zijn internetsite wordt bezocht, voor deze aanbieder een persoonsgegeven vormt.

Het Hof heeft er om te beginnen op gewezen dat voor de kwalificatie van een gegeven als „persoonsgegeven" in de zin van artikel 2, onder a), van richtlijn 95/46 niet vereist is dat alle informatie aan de hand waarvan de betrokkene kan worden geïdentificeerd, bij een en dezelfde persoon berust. Dat de extra informatie die nodig is om de gebruiker van een website te identificeren, niet berust bij de aanbieder van onlinemediadiensten, maar bij de internetprovider van deze gebruiker, lijkt dan ook niet uit te sluiten dat dynamische IP-adressen die worden geregistreerd door deze aanbieder, voor hem persoonsgegevens vormen in de zin van artikel 2, onder a), van richtlijn 95/46 (punten 43 en 44).

Bijgevolg heeft het Hof vastgesteld dat een dynamisch IP-adres dat door een aanbieder van onlinemediadiensten wordt geregistreerd telkens wanneer een persoon een website bezoekt die door deze aanbieder toegankelijk wordt gemaakt voor het publiek, ten aanzien van die aanbieder een persoonsgegeven in de zin van artikel 2, onder a), van richtlijn 95/46 vormt, wanneer hij beschikt over wettige middelen waarmee hij de betrokken persoon kan identificeren aan de hand van extra informatie over die persoon die bij de internetprovider van deze persoon berust (punt 49 en dictum 1).

Arrest van 20 december 2017, Nowak (C-434/16, EU:C:2017:994)

Nowak, een stagiair-accountant, was niet geslaagd voor het door de Ierse beroepsorganisatie van accountants georganiseerde examen. Hij diende op grond van artikel 4 van de wet gegevensbescherming een verzoek in om toegang te verkrijgen tot alle hem betreffende persoonsgegevens waarover de beroepsorganisatie van accountants beschikte. Deze beroepsorganisatie heeft Nowak bepaalde documenten toegezonden maar weigerde diens schriftelijk examenwerk vrij te geven, met als argument dat dit geen persoonsgegevens in de zin van de wet gegevensbescherming bevatte.

Daar ook de toezichthouder voor de gegevensbescherming om dezelfde redenen geen gevolg gaf aan Nowaks verzoek om toegang, heeft Nowak zich tot de nationale rechterlijke instanties gewend. De Supreme Court (hoogste rechterlijke instantie, Ierland), waarbij Nowak een hogere voorziening had ingesteld, heeft het Hof de vraag voorgelegd of artikel 2, onder a), van richtlijn 95/46 aldus moet worden uitgelegd dat, in omstandigheden als die in het hoofdgeding, de door een kandidaat geformuleerde schriftelijke antwoorden op een beroepsexamen en de eventuele opmerkingen van de examinator bij deze antwoorden de kandidaat betreffende persoonsgegevens zijn in de zin van deze bepaling.

In de eerste plaats heeft het Hof erop gewezen dat voor de kwalificatie van een gegeven als „persoonsgegeven" in de zin van artikel 2, onder a), van richtlijn 95/46 niet vereist is dat alle

informatie aan de hand waarvan de betrokkene kan worden geïdentificeerd, bij een en dezelfde persoon berust. Bovendien, ingeval de examinator de identiteit van de kandidaat niet kent op het moment van de markering van de door de kandidaat verstrekte examenantwoorden, beschikt de instantie die het examen organiseert – in casu de beroepsorganisatie van accountants – wel degelijk over de nodige informatie die deze instantie toelaat om de kandidaat zonder problemen of twijfels te identificeren aan de hand van het identificatienummer dat op zijn examenwerk of op de omslag ervan is aangebracht, en om zijn antwoorden aan hem toe te schrijven.

In de tweede plaats heeft het Hof vastgesteld dat de door een kandidaat op een beroepsexamen geformuleerde schriftelijke antwoorden voor hem persoonsgebonden informatie vormen. De inhoud van deze antwoorden weerspiegelt namelijk het niveau van de kennis en de vaardigheden van de kandidaat op een welbepaald gebied, en eventueel ook zijn gedachtegang, oordeel en kritische geest. Voorts heeft het verzamelen van de voormelde antwoorden tot doel een evaluatie te maken van de beroepsbekwaamheden van de kandidaat en diens geschiktheid om het betrokken beroep uit te oefenen. Daarnaast kan het gebruik van deze informatie, dat met name leidt tot het al dan niet slagen van de kandidaat voor het betrokken examen, gevolgen hebben voor zijn rechten en belangen, aangezien het bijvoorbeeld zijn kansen om in aanmerking te komen voor het gewenste beroep of de gewenste functie kan bepalen of beïnvloeden. De vaststelling dat de door een kandidaat geformuleerde schriftelijke antwoorden op een beroepsexamen informatie betreffende deze kandidaat vormen vanwege hun inhoud, doel of gevolg, geldt trouwens evenzeer wanneer het om een openboekexamen gaat (punten 31 en 36-40).

Wat in de derde plaats de opmerkingen van de examinator bij de examenantwoorden van de kandidaat betreft, moet worden vastgesteld dat deze, net als de antwoorden van de kandidaat, informatie betreffende deze laatste vormen, daar zij immers de mening of beoordeling van de examinator weergeven betreffende de individuele prestaties van de kandidaat tijdens het examen, en meer bepaald betreffende diens kennis en vaardigheden op het betrokken gebied. Die opmerkingen hebben overigens juist tot doel om de evaluatie door de examinator van de prestaties van de kandidaat vast te leggen, en kunnen voor deze laatste effecten sorteren (punten 42 en 43).

In de vierde plaats heeft het Hof geoordeeld dat de door een kandidaat geformuleerde schriftelijke antwoorden op een beroepsexamen en de eventuele opmerkingen van de examinator bij deze antwoorden kunnen worden getoetst op, onder meer, hun juistheid en de noodzaak om te worden bewaard in de zin van artikel 6, lid 1, onder d) en e), van richtlijn 95/46, alsook het voorwerp kunnen uitmaken van een rectificatie of uitwissing uit hoofde van artikel 12, onder b), van deze richtlijn. Het verlenen van een recht op toegang tot die antwoorden en opmerkingen krachtens artikel 12, onder a), van deze richtlijn dient het doel van die richtlijn dat erin bestaat de bescherming te garanderen van het recht op de persoonlijke levenssfeer van de kandidaat in verband met de verwerking van zijn persoonsgegevens, ongeacht of die kandidaat een dergelijk recht op toegang heeft krachtens de op de examenprocedure van toepassing zijnde nationale wetgeving. Het Hof heeft evenwel beklemtoond dat de rechten van toegang en van rectificatie die aan artikel 12, onder a) en b), van richtlijn 95/46 kunnen worden ontleend, zich niet uitstrekken tot de examenvragen, aangezien deze als zodanig geen persoonsgegevens van de kandidaat vormen (punten 56 en 58).

Gelet op deze aspecten kwam het Hof tot de slotsom dat in omstandigheden als die van het hoofdgeding de door de kandidaat geformuleerde schriftelijke antwoorden op een beroepsexamen en de eventuele opmerkingen van de examinator bij deze antwoorden, persoonsgegevens in de zin van artikel 2, onder a), van richtlijn 95/46 vormen (punt 62 en dictum).

3. Begrip „verwerking van persoonsgegevens"

Arrest van 6 november 2003 (Grote kamer), Lindqvist (C-101/01, EU:C:2003:596)

Lindqvist, vrijwilligster bij een gemeente van de Protestantse Kerk van Zweden, had op haar eigen computer internetpagina's gecreëerd en daarop persoonsgegevens gepubliceerd over verschillende personen die net zoals zij als vrijwilliger werkten binnen die gemeente. Lindqvist werd veroordeeld tot betaling van een geldboete omdat zij in het kader van een geautomatiseerde gegevensverwerking persoonsgegevens had gebruikt zonder dit vooraf schriftelijk aan de Zweedse Datainspektion (overheidsorgaan voor de bescherming van elektronisch doorgegeven gegevens) te melden, deze gegevens zonder toestemming naar derde landen had doorgegeven en gevoelige persoonsgegevens had verwerkt.

In het hoger beroep van Lindqvist bij de Göta hovrätt (rechter in tweede aanleg, Zweden) tegen deze beslissing, heeft die rechterlijke instantie het Hof verzocht om een prejudiciële beslissing, met name om te vernemen of Lindqvist een „geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens" in de zin van richtlijn 95/46 had verricht.

Het Hof heeft vastgesteld dat het vermelden van verschillende personen op een internetpagina met hun naam of anderszins, bijvoorbeeld met hun telefoonnummer of informatie over hun werksituatie en hun liefhebberijen, als een „geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens" in de zin van deze richtlijn is aan te merken (punt 27 en dictum 1). Een dergelijke verwerking van persoonsgegevens die geschiedt met het oog op het verrichten van vrijwilligerswerk of religieuze activiteiten, valt immers niet onder een van de uitzonderingen op de werkingssfeer van de richtlijn, daar die verwerking noch behoort tot de categorie van activiteiten die betrekking hebben op de openbare veiligheid noch tot de categorie van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden, die buiten de werkingssfeer van de richtlijn vallen (punten 38, 43-48 en dictum 2).

Arrest van 13 mei 2014 (Grote kamer), Google Spain en Google (C-131/12, EU:C:2014:317)

In 2010 had een Spaans staatsburger bij de Agencia Española de Protección de Datos (Spaans agentschap voor de gegevensbescherming; hierna: „AEPD") een klacht ingediend tegen La Vanguardia Ediciones SL, uitgeefster van een dagblad met grote oplage in Spanje, alsmede tegen Google Spain en Google. Deze persoon voerde aan dat wanneer een internetgebruiker zijn naam ingaf in de zoekmachine van het Googleconcern, er koppelingen verschenen naar twee pagina's van het dagblad *La Vanguardia* uit 1998, waarin met name een verkoop per opbod van gebouwen werd aangekondigd waarmee zijn schulden moesten worden gedekt. Met zijn klacht verzocht deze persoon ten eerste dat La Vanguardia Ediciones werd gelast hetzij de betrokken pagina's te verwijderen of te wijzigen hetzij deze gegevens te beschermen via

bepaalde door de zoekmachines geboden instrumenten. Ten tweede verzocht deze persoon dat Google Spain of Google werd gelast zijn persoonsgegevens te verwijderen of te maskeren, zodat deze zouden verdwijnen uit de zoekresultaten en uit de koppelingen van La Vanguardia Ediciones.

De AEPD had de klacht tegen La Vanguardia Ediciones afgewezen, daar hij meende dat de betrokken informatie door de redacteur rechtmatig was gepubliceerd, maar had daarentegen de klacht jegens Google Spain en Google gegrond verklaard en deze twee ondernemingen verzocht de nodige maatregelen te nemen om de gegevens uit hun index te verwijderen en voor de toekomst de toegang tot deze gegevens onmogelijk te maken. Daar deze ondernemingen bij de Audiencia Nacional (nationale centrale rechterlijke instantie, Spanje) elk beroep hadden ingesteld tot nietigverklaring van de beslissing van de AEPD, heeft deze Spaanse rechterlijke instantie het Hof een reeks vragen voorgelegd.

Het Hof kreeg dus de gelegenheid om het begrip „verwerking van persoonsgegevens" op internet nader te bepalen in het licht van richtlijn 95/46.

Het Hof heeft aldus geoordeeld dat de activiteit van een zoekmachine, die erin bestaat door derden op het internet gepubliceerde of opgeslagen informatie te vinden, automatisch te indexeren, tijdelijk op te slaan en, ten slotte, in een bepaalde volgorde ter beschikking te stellen aan internetgebruikers, moet worden gekwalificeerd als verwerking van persoonsgegevens wanneer deze informatie persoonsgegevens bevat (dictum 1). Het Hof heeft voorts in herinnering gebracht dat ook wanneer de in de richtlijn bedoelde verrichtingen uitsluitend betrekking hebben op informatie die reeds ongewijzigd in de media is gepubliceerd, zij als verwerking moeten worden aangemerkt. Een algemene afwijking van de toepassing van de richtlijn in een dergelijke hypothese zou deze richtlijn grotendeels zinloos maken (punten 29 en 30).

Arrest van 10 juli 2018 (Grote kamer), Jehovan todistajat (C-25/17, EU:C:2018:551)[20]

De Finse gegevensbeschermingsautoriteit had een besluit vastgesteld waarbij aan de gemeenschap van Jehova's getuigen werd verboden om in het kader van de van-huis-tot-huisverkondiging door haar leden persoonsgegevens te verzamelen en te verwerken zonder de in de Finse wettelijke regeling betreffende de verwerking van persoonsgegevens gestelde voorwaarden in acht te nemen. De leden van deze gemeenschap maken in het kader van hun van-huis-tot-huisverkondiging immers aantekeningen over de bezoeken die zij hebben gebracht aan personen die zijzelf of die gemeenschap niet kennen. Deze gegevens worden verzameld als geheugensteun om gemakkelijk te kunnen worden teruggevonden voor een eventueel later bezoek, zonder dat de betrokken personen daarmee hebben ingestemd of daarvan op de hoogte zijn gebracht. In dit verband heeft de gemeenschap van Jehova's getuigen haar leden richtsnoeren gegeven voor het maken van dergelijke aantekeningen. Deze richtsnoeren zijn terug te vinden in ten minste één van de aan de verkondigingsactiviteit gewijde tijdschriften van deze gemeenschap.

[20] Dit arrest is opgenomen in het Jaarverslag 2018, blz. 91 en 92.

Het Hof heeft geoordeeld dat het verzamelen van persoonsgegevens door leden van een geloofsgemeenschap in het kader van een van-huis-tot-huisverkondiging en de latere verwerking van die gegevens niet behoren tot de situaties waarin richtlijn 95/46 niet van toepassing is, aangezien zij geen verwerking van persoonsgegevens met het oog op de uitoefening van activiteiten als bedoeld in artikel 3, lid 2, eerste streepje, van deze richtlijn vormen en evenmin een verwerking van persoonsgegevens die door natuurlijke personen in een activiteit met uitsluitend persoonlijke of huishoudelijke doeleinden wordt verricht in de zin van artikel 3, lid 2, tweede streepje, van deze richtlijn (punt 51 en dictum 1).

Arrest van 14 februari 2019, Buivids (C-345/17, EU:C:2019:122)

In deze zaak is het Hof ingegaan op, ten eerste, de werkingssfeer van richtlijn 95/46 en, ten tweede, de uitlegging van het in artikel 9 van deze richtlijn bedoelde begrip „verwerking van persoonsgegevens voor uitsluitend journalistieke doeleinden".

Dit arrest is gewezen in het kader van een verzoek om een prejudiciële beslissing dat was ingediend door de hoogste rechterlijke instantie van Letland, waarbij een geding aanhangig was tussen Buivids (hierna: „verzoeker") en de nationale gegevensbeschermingsautoriteit over een beroep tot onrechtmatigverklaring van een door deze autoriteit vastgesteld besluit volgens hetwelk verzoeker de nationale wetgeving inzake de bescherming van persoonsgegevens had geschonden door op een website een zelf opgenomen video te plaatsen waarop was te zien hoe hij tegenover politieagenten op een politiebureau van de nationale politie in het kader van een administratieve procedure wegens een overtreding een verklaring aflegt. Nadat zijn beroep door twee lagere rechters was verworpen stelde verzoeker bij de hoogste rechterlijke instantie cassatieberoep in. Bij deze rechter beriep hij zich op zijn recht op vrijheid van meningsuiting en voerde hij aan dat op de betrokken video politieagenten van de nationale politie te zien waren, die publieke personen zijn op een voor het publiek toegankelijke plaats en dat deze personen daardoor geen aanspraak konden maken op toepassing van de bepalingen van de wet inzake de bescherming van persoonsgegevens.

Wat in de eerste plaats de werkingssfeer van richtlijn 95/46 betreft, heeft het Hof opgemerkt dat, ten eerste, de op de betrokken video opgenomen beelden van de politieagenten persoonsgegevens vormen, en, ten tweede, het opnemen van videobeelden van deze personen die worden vastgelegd in het geheugen van de door verzoeker gebruikte camera, een verwerking van persoonsgegevens vormt. Het Hof heeft daaraan toegevoegd dat wanneer een video-opname waarop persoonsgegevens te zien zijn, wordt gepubliceerd op een website waarop gebruikers video's kunnen plaatsen, bekijken en delen, dit dus een geheel of gedeeltelijk geautomatiseerde verwerking van die gegevens vormt. Bovendien heeft het Hof beklemtoond dat die opname en de publicatie ervan niet vallen onder de uitzonderingen op de werkingssfeer van richtlijn 95/46, betreffende met name de verwerking van persoonsgegevens die geschiedt in het kader van activiteiten die niet binnen de werkingssfeer van deze richtlijn vallen en verwerkingen in het kader van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden. Bijgevolg kwam het Hof tot de slotsom dat een video-opname van politieagenten die op een politiebureau aanwezig zijn terwijl daar een verklaring wordt afgelegd, en de publicatie van de opgenomen beelden op een website waarop gebruikers video's kunnen plaatsen, bekijken en delen, binnen de werkingssfeer van deze richtlijn vallen (punten 31, 32, 35, 39, 42, 43 en dictum 1).

Wat in de tweede plaats de strekking van het begrip „verwerking van persoonsgegevens voor uitsluitend journalistieke doeleinden" betreft, heeft het Hof om te beginnen in herinnering gebracht dat volgens een ruime uitlegging van het begrip „journalistiek" de in artikel 9 van richtlijn 95/46 bedoelde ontheffingen en uitzonderingen gelden voor alle personen die journalistieke activiteiten ontplooien. Aldus heeft het Hof geoordeeld dat het feit dat verzoeker geen professioneel journalist was, niet uitsloot dat de betrokken video-opname en het doorzenden ervan konden worden gekwalificeerd als „verwerking van persoonsgegevens voor uitsluitend journalistieke doeleinden". Bovendien heeft het Hof beklemtoond dat de in artikel 9 van richtlijn 95/46 bedoelde ontheffingen en uitzonderingen alleen mogen worden toegepast voor zover zij nodig blijken om twee fundamentele rechten te verzoenen, namelijk bescherming van de persoonlijke levenssfeer en de vrijheid van meningsuiting. In dit verband heeft het Hof gepreciseerd dat niet is uitgesloten dat bij de opname en de publicatie van de betrokken video zonder dat de politieagenten op deze video over deze opname en het doel ervan waren geïnformeerd, sprake is van inmenging in hun fundamentele recht op eerbiediging van de persoonlijke levenssfeer. Bijgevolg heeft het Hof geconcludeerd dat er bij de betrokken video-opname en het plaatsen ervan op een website sprake kan zijn van verwerking van persoonsgegevens voor uitsluitend journalistieke doeleinden, voor zover uit die video valt af te leiden dat het doel van de opname en van de publicatie uitsluitend erin bestond informatie, meningen of ideeën aan het publiek bekend te maken, hetgeen aan de verwijzende rechterlijke instantie staat om na te gaan (punten 51, 52, 55, 63, 67 en dictum 2).

Arrest van 22 juni 2021 (Grote kamer), Latvijas Republikas Saeima (Strafpunten) (C-439/19, EU:C:2021:504)

B is een natuurlijke persoon aan wie strafpunten zijn toegekend wegens een of meer verkeersovertredingen. De Ceļu satiksmes drošības direkcija (directie verkeersveiligheid, Letland; hierna: „CSDD") heeft deze strafpunten aangetekend in het nationale register van voertuigen en de bestuurders daarvan.

Op grond van de Letse regeling inzake het wegverkeer[21] is informatie over de aan bestuurders van voertuigen toegekende strafpunten die zijn aangetekend in dat register, toegankelijk voor het publiek en wordt zij door de CSDD verstrekt aan eenieder die erom verzoekt – onder meer aan marktdeelnemers die deze informatie willen hergebruiken – zonder dat de aanvrager hoeft aan te tonen dat hij een specifiek belang heeft bij het verkrijgen van die informatie. Aangezien B twijfelt aan de rechtmatigheid van deze regeling, heeft hij bij de Latvijas Republikas Satversmes tiesa (grondwettelijk hof, Letland; hierna: „verwijzende rechter") een beroep tot constitutionele toetsing ingesteld om te laten onderzoeken of die regeling in overeenstemming is met het recht op eerbiediging van het privéleven.

Het grondwettelijk hof heeft geoordeeld dat het bij zijn beoordeling van dit constitutionele recht rekening moet houden met de AVG. Hij heeft het Hof dan ook verzocht om de draagwijdte van verschillende bepalingen van de AVG te verduidelijken teneinde vast te stellen of de Letse regeling inzake het wegverkeer verenigbaar is met die verordening.

In zijn arrest, gewezen door de Grote kamer, heeft het Hof geoordeeld dat de verwerking van persoonsgegevens die betrekking hebben op strafpunten een „verwerking van

[21] Artikel 14[1], lid 2, van de Ceļu satiksmes likums (wet betreffende het wegverkeer) van 1 oktober 1997 (*Latvijas Vēstnesis*, 1997, nr. 274/276).

persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten"[22] is, waarvoor de AVG meer bescherming biedt omdat de gegevens in kwestie bijzonder gevoelig zijn (punten 10, 46, 74, 94 en dictum 1).

In dit verband merkt het Hof om te beginnen op dat het bij informatie over strafpunten gaat om persoonsgegevens en dat de verstrekking door de CSDD van deze gegevens aan derden een verwerking is die binnen de materiële werkingssfeer van de AVG valt. De werkingssfeer van deze verordening is namelijk zeer ruim en die verwerking valt niet onder de uitzonderingen op de toepasselijkheid van die verordening (punten 60, 61 en 72).

Ten eerste valt de verwerking van de persoonsgegevens in kwestie niet onder de uitzondering die inhoudt dat de AVG niet toepasselijk is op een verwerking in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen.[23] Aangenomen moet worden dat deze uitzondering enkel tot doel heeft de verwerking van persoonsgegevens uit te sluiten van de werkingssfeer van die verordening wanneer de betreffende persoonsgegevens worden verwerkt door overheidsinstanties in het kader van activiteiten die ertoe strekken de nationale veiligheid te beschermen of in het kader van activiteiten die in dezelfde categorie kunnen worden ondergebracht. Daarbij gaat het met name om activiteiten die tot doel hebben de essentiële functies van de staat en de fundamentele belangen van de samenleving te beschermen. Met activiteiten die verband houden met verkeersveiligheid wordt een dergelijke doelstelling niet nagestreefd, zodat deze activiteiten niet kunnen worden gerekend tot de categorie van activiteiten die ertoe strekken de nationale veiligheid te beschermen (punten 62 en 66-68).

Ten tweede is de verstrekking van persoonsgegevens betreffende strafpunten evenmin een verwerking die valt onder de uitzondering op grond waarvan de AVG niet geldt voor de verwerking van persoonsgegevens door de op het gebied van strafzaken bevoegde autoriteiten.[24] Het Hof stelt namelijk vast dat de CSDD bij het verstrekken van die gegevens niet kan worden aangemerkt als een „bevoegde autoriteit"[25] in die zin (punten 69-71).

Voorts onderzoekt het Hof of de toegang tot persoonsgegevens betreffende verkeersovertredingen, zoals strafpunten, een verwerking vormt van persoonsgegevens betreffende „strafbare feiten"[26], die een ruimere bescherming genieten. In dit verband constateert het Hof dat dit begrip uitsluitend betrekking heeft op strafbare feiten in strafrechtelijke zin. Hiervoor baseert het Hof zich met name op de totstandkomingsgeschiedenis van de AVG. Dat verkeersovertredingen in het Letse rechtsstelsel worden gekwalificeerd als bestuursrechtelijk bestrafte overtredingen, is evenwel niet beslissend voor de beoordeling of deze overtredingen onder het begrip „strafbaar feit" in strafrechtelijke zin vallen, aangezien het gaat om een autonoom Unierechtelijk begrip dat in de gehele Unie autonoom en uniform moet worden uitgelegd. Nadat het Hof de drie criteria in herinnering heeft gebracht die relevant zijn om te beoordelen of een strafbaar feit van strafrechtelijke aard is – te weten de juridische kwalificatie van het strafbare feit naar nationaal recht, de aard van het strafbare feit en de

22 Artikel 10 AVG.
23 Artikel 2, lid 2, onder a), AVG.
24 Artikel 2, lid 2, onder d), AVG.
25 Artikel 3, punt 7, van 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 (PB 2016, L 119, blz. 89).
26 Artikel 10 AVG.

zwaarte van de sanctie die kan worden opgelegd – oordeelt het dat de verkeersovertredingen in kwestie onder het begrip „strafbaar feit" in de zin van de AVG vallen. Wat de eerste twee criteria betreft, stelt het Hof vast dat zelfs bij strafbare feiten die naar nationaal recht niet als strafbare feiten in strafrechtelijke zin worden gekwalificeerd, uit de aard van het strafbare feit en met name uit het repressieve doel van de sanctie die daarvoor kan worden opgelegd, kan voortvloeien dat het om dergelijke feiten gaat. In het onderhavige geval wordt met de toekenning van strafpunten wegens verkeersovertredingen – net zoals met de andere sancties die wegens verkeersovertredingen kunnen worden opgelegd – onder meer een dergelijk repressief doel nagestreefd. Met betrekking tot het derde criterium merkt het Hof op dat alleen verkeersovertredingen van enige ernst tot gevolg hebben dat er strafpunten worden toegekend, zodat dergelijke overtredingen kunnen leiden tot sancties van enige zwaarte. Tevens komt de toekenning van strafpunten doorgaans boven op de opgelegde sanctie en heeft de accumulatie van strafpunten rechtsgevolgen, die zelfs kunnen gaan tot een rijverbod (punten 77, 80, 85, 87-90 en 93).

4. Begrip „bestand van persoonsgegevens"

Arrest van 10 juli 2018 (Grote kamer), Jehovan todistajat (C-25/17, EU:C:2018:551)

In dit arrest (zie tevens rubriek II.3, met het opschrift „Begrip ‚verwerking van persoonsgegevens'"), heeft het Hof het begrip „bestand" in de zin van artikel 2, onder c), van richtlijn 95/46 nader bepaald.

Zo heeft het Hof – na in herinnering te hebben gebracht dat deze richtlijn slechts op de niet-geautomatiseerde verwerking van persoonsgegevens van toepassing is indien de verwerkte gegevens worden of zullen worden opgenomen in een bestand – geoordeeld dat onder dit begrip ook valt een geheel van in het kader van een van-huis-tot-huisverkondiging verzamelde persoonsgegevens, bestaande uit de naam en het adres van en andere informatie over de aan huis bezochte personen, wanneer deze gegevens zijn gestructureerd volgens specifieke criteria die het in de praktijk mogelijk maken deze gegevens gemakkelijk terug te vinden voor later gebruik ervan. Om onder dit begrip te vallen hoeft een dergelijk geheel geen steekkaarten, specifieke lijsten of andere ordeningssystemen te omvatten (punt 62 en dictum 2).

5. Begrip „voor de verwerking van persoonsgegevens verantwoordelijke"

Arrest van 10 juli 2018 (Grote kamer), Jehovan todistajat (C-25/17, EU:C:2018:551)

In deze zaak (zie tevens de rubrieken II.3 en II.4, met de opschriften „Begrip ‚verwerking van persoonsgegevens'" respectievelijk „Begrip ‚bestand van persoonsgegevens'") heeft het Hof zich uitgesproken over de verantwoordelijkheid van een geloofsgemeenschap voor de verwerking van persoonsgegevens die plaatsvindt in het kader van de door deze gemeenschap georganiseerde, gecoördineerde en aangemoedigde van-huis-tot-huisverkondiging.

Zo was het Hof van oordeel dat de verplichting voor eenieder om de regels van het Unierecht betreffende de bescherming van persoonsgegevens in acht te nemen, niet als een inmenging in de organisatieautonomie van die gemeenschappen kan worden beschouwd. Het Hof is in dit

verband tot de slotsom gekomen dat artikel 2, onder d), van richtlijn 95/46, gelezen tegen de achtergrond van artikel 10, lid 1, van het Handvest, in die zin moet worden uitgelegd dat een geloofsgemeenschap samen met haar leden-verkondigers kan worden beschouwd als verantwoordelijke voor de verwerking van de persoonsgegevens die laatstgenoemden in het kader van een door deze gemeenschap georganiseerde, gecoördineerde en aangemoedigde van-huis-tot-huisverkondiging verrichten, zonder dat daartoe nodig is dat die gemeenschap toegang heeft tot die gegevens of dat wordt aangetoond dat zij haar leden schriftelijke richtsnoeren of instructies voor die verwerking heeft gegeven (punten 74, 75 en dictum 3).

Arrest van 5 juni 2018 (Grote kamer), Wirtschaftsakademie Schleswig Holstein (C-210/16, EU:C:2018:388)[27]

De Duitse autoriteit voor de bescherming van persoonsgegevens had, in haar hoedanigheid van toezichthoudende autoriteit in de zin van artikel 28 van richtlijn 95/46, een Duitse vennootschap die was gespecialiseerd op het gebied van onderwijs en die onderwijsdiensten aanbood door middel van een fanpagina op het sociale netwerk Facebook, gelast haar fanpagina te deactiveren. Volgens die autoriteit had immers noch deze vennootschap, noch Facebook de bezoekers van de fanpagina ervan op de hoogte gebracht dat Facebook door middel van cookies persoonlijke informatie over hen verzamelde en dat genoemde vennootschap en Facebook deze informatie vervolgens verwerkten.

In deze context heeft het Hof het begrip „verantwoordelijke voor de verwerking van persoonsgegevens" nader bepaald. Het Hof heeft in dit verband vastgesteld dat de beheerder van een op Facebook geplaatste fanpagina, zoals de vennootschap in het hoofdgeding, door het vastleggen van instellingen (naargelang van, met name, zijn doelpubliek en van doelstellingen voor het beheer of de promotie van zijn activiteiten) deelneemt aan de vaststelling van het doel van en de middelen voor de verwerking van de persoonsgegevens van de bezoekers van zijn fanpagina. Derhalve moet deze beheerder volgens het Hof worden aangemerkt als verantwoordelijke binnen de Unie, gezamenlijk met Facebook Ireland (de dochteronderneming, in de Unie, van de Amerikaanse vennootschap Facebook), voor deze verwerking, in de zin van artikel 2, onder d), van richtlijn 95/46 (punt 39).

Arrest van 29 juli 2019, Fashion ID (C-40/17, EU:C:2019:629)

Deze zaak bood het Hof de gelegenheid het begrip „voor de verwerking verantwoordelijke" verder uit te werken in het licht van de integratie van een plug-in in een website.

In casu had Fashion ID, een Duitse onlinehandelaar in modekleding, op haar internetsite de social plug-in „vind-ik-leuk" van het sociale netwerk Facebook ingevoegd. Deze invoeging had tot gevolg dat wanneer een bezoeker de internetsite van Fashion ID raadpleegde, persoonsgegevens van deze bezoeker naar Facebook Ireland werden doorgezonden. Het doorzenden van die persoonsgegevens vond kennelijk plaats zonder dat die bezoeker zich daarvan bewust was en ongeacht of hij al dan niet lid was van het sociale netwerk Facebook of op de vind-ik-leukknop van Facebook had geklikt.

[27] Dit arrest is opgenomen in het Jaarverslag 2018, blz. 91.

De Verbraucherzentrale NRW, een Duitse vereniging van algemeen nut die consumentenbelangen behartigt, verweet Fashion ID persoonsgegevens van de bezoekers van de Fashion ID-internetsite aan Facebook Ireland te hebben doorgezonden zonder de toestemming van die bezoekers en in strijd met de verplichtingen die in de bepalingen inzake de bescherming van persoonsgegevens zijn neergelegd met betrekking tot het verstrekken van informatie. Het Oberlandesgericht Düsseldorf (hoogste rechterlijke instantie van de deelstaat Noordrijn-Westfalen, Düsseldorf, Duitsland), waarbij het geding aanhangig was gemaakt, verzocht het Hof om uitlegging van een aantal bepalingen van richtlijn 95/46.

Het Hof heeft om te beginnen vastgesteld dat de beheerder van een internetsite, zoals Fashion ID, kan worden geacht voor de verwerking verantwoordelijk te zijn in de zin van artikel 2, onder d), van richtlijn 95/46. Deze verantwoordelijkheid is evenwel beperkt tot de bewerking of het geheel van bewerkingen op het gebied van de verwerking van persoonsgegevens waarvan respectievelijk waarvoor hij daadwerkelijk het doel en de middelen vaststelt, te weten het verzamelen en door middel van doorzending verstrekken van de gegevens in kwestie. Volgens het Hof leek het op het eerste gezicht evenwel uitgesloten dat Fashion ID het doel en de middelen van respectievelijk voor bewerkingen vaststelde die verband houden met de verwerking van persoonsgegevens en die door Facebook Ireland werden uitgevoerd op een later tijdstip, nadat haar de betreffende gegevens waren doorgezonden, zodat Fashion ID niet kon worden geacht voor die bewerkingen verantwoordelijk te zijn in de zin van genoemd artikel 2, onder d) (punten 76, 85 en dictum 2).

Voorts heeft het Hof beklemtoond dat die verwerkingshandelingen van de beheerder van een internetsite en van de aanbieder van een social plug-in, zoals Facebook Ireland, enkel gerechtvaardigd zijn indien elk van hen daarmee een legitiem belang behartigt in de zin van artikel 7, onder f), van richtlijn 95/46 (punt 97 en dictum 3).

Ten slotte heeft het Hof gepreciseerd dat de in artikel 2, onder h), en artikel 7, onder a), van richtlijn 95/46 bedoelde toestemming van de betrokkene door de beheerder van een website enkel moet worden verkregen voor bewerkingen op het gebied van de verwerking van persoonsgegevens waarvan respectievelijk waarvoor hij het doel en de middelen vaststelt. In een dergelijke situatie rust ook de in artikel 10 van die richtlijn vastgelegde verplichting tot informatieverstrekking op die beheerder, zij het dat de door hem aan de betrokkene te verstrekken informatie enkel betrekking dient te hebben op de bewerking of het geheel van bewerkingen op het gebied van de verwerking van persoonsgegevens waarvan respectievelijk waarvoor hij daadwerkelijk het doel en de middelen vaststelt (punt 106 en dictum 4).

Arrest van 9 juli 2020, Land Hessen, C-272/19, EU:C:2020:535

Een burger die bij de Commissie verzoekschriften van de Hessische Landtag (parlement van de deelstaat Hessen, Duitsland) een verzoekschrift had ingediend, heeft deze commissie verzocht om inzage van de hem betreffende persoonsgegevens, die deze commissie in het kader van de behandeling van zijn verzoekschrift had bewaard. Hij baseert zich voor dit verzoek op de AVG, die voorziet in het recht van een betrokkene om van de verwerkingsverantwoordelijke inzage te verkrijgen van de hem betreffende persoonsgegevens.

De voorzitter van de Hessische Landtag heeft dit verzoek afgewezen op grond dat de verzoekschriftenprocedure een taak van het parlement is, en dat dit parlement niet onder de AVG valt.

Het Verwaltungsgericht Wiesbaden (bestuursrechter Wiesbaden, Duitsland), waartoe de burger zich heeft gewend, is van oordeel dat het Duitse recht geen recht op inzage van persoonsgegevens toekent in het kader van een verzoekschrift als dat in het geding. Het Verwaltungsgericht Wiesbaden is echter van mening dat een dergelijk recht van inzage kan voortvloeien uit de AVG en heeft het Hof van Justitie hierover vragen gesteld. Bovendien heeft het Verwaltungsgericht Wiesbaden twijfels over zijn eigen onafhankelijkheid en dus over zijn hoedanigheid van rechterlijke instantie, die het Hof prejudiciële vragen mag voorleggen, en heeft het derhalve ook hierover vragen gesteld aan het Hof.

In zijn arrest antwoordt het Hof dat een commissie verzoekschriften van het parlement van een deelstaat van een lidstaat, voor zover zij, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt, moet worden aangemerkt als „verwerkingsverantwoordelijke" in de zin van de AVG[28]. De verwerking van persoonsgegevens door een dergelijke commissie valt dus onder deze verordening, met name onder de bepaling die de betrokkenen een recht van inzage van de hen betreffende persoonsgegevens verleent[29].

Het Hof stelt met name vast dat de activiteiten van de commissie verzoekschriften van de Hessische Landtag niet onder een in de AVG geregelde uitzondering vallen. Hoewel het Hof erkent dat dergelijke activiteiten van publieke aard zijn en specifiek zijn aan deze deelstaat, aangezien deze commissie indirect bijdraagt tot de parlementaire activiteit, merkt het op dat deze activiteiten tevens van politieke en bestuurlijke aard zijn. Bovendien blijkt uit de gegevens waarover het Hof beschikt geenszins dat die activiteiten in casu overeenkomen met een van de uitzonderingen waarin de AVG voorziet (punten 71-74 en dictum).

6. Voorwaarden waaronder een verwerking van persoonsgegevens rechtmatig is

Arrest van 16 december 2008 (Grote kamer), Huber (C-524/06, EU:C:2008:724)[30]

Het federaal bureau voor migratie en vluchtelingen (Bundesamt für Migration und Flüchtlinge, Duitsland) was belast met het beheer van een centraal vreemdelingenregister waarin bepaalde persoonsgegevens waren opgenomen betreffende buitenlanders die langer dan drie maanden op het Duitse grondgebied verblijven. Dit register werd gebruikt voor statistiekdoeleinden en bij de uitoefening door veiligheids- en politiepersoneel en door rechterlijke autoriteiten van opsporings- en onderzoeksbevoegdheden ter zake van strafbare feiten of handelingen die de openbare veiligheid in gevaar brengen.

28 Artikel 4, punt 7, AVG.
29 Artikel 15 AVG.
30 Dit arrest is opgenomen in het Jaarverslag 2008, blz. 46.

Huber, Oostenrijks staatsburger, had zich in 1996 in Duitsland gevestigd om daar als zelfstandig verzekeringsagent te werken. Daar hij van mening was dat de verwerking van zijn in het betrokken register opgenomen gegevens discriminatie vormde, omdat een dergelijk bestand voor Duitse burgers niet bestond, heeft Huber om verwijdering van deze gegevens verzocht.

In deze context heeft het in die zaak aangezochte Oberverwaltungsgericht für das Land Nordrhein-Westfalen (hoogste bestuursrechter van de deelstaat Noordrijn-Westfalen, Duitsland), het Hof gevraagd of de verwerking van persoonsgegevens die in het betrokken register plaatsvond, verenigbaar was met het Unierecht.

Het Hof heeft om te beginnen in herinnering gebracht dat het verblijfsrecht van een Unieburger op het grondgebied van een lidstaat waarvan hij niet de nationaliteit bezit, niet onvoorwaardelijk is, maar kan worden gebonden aan beperkingen. Het gebruik van een dergelijk register voor de ondersteuning van de met de uitvoering van de verblijfswetgeving belaste autoriteiten is dus in beginsel legitiem en, gelet op het karakter van dit register, verenigbaar met het in artikel 12, lid 1, EG (thans artikel 18, eerste alinea, VWEU) neergelegde verbod van discriminatie op grond van nationaliteit. Een dergelijk register mag echter geen andere informatie bevatten dan voor dat doel noodzakelijk is, in de zin van de richtlijn betreffende de bescherming van persoonsgegevens (punten 54, 58 en 59).

Wat het begrip „noodzaak" van de verwerking in de zin van artikel 7, onder e), van richtlijn 95/46 betreft, heeft het Hof allereerst in herinnering gebracht dat het gaat om een autonoom begrip van het Unierecht, dat moet worden uitgelegd op een wijze die volledig beantwoordt aan het doel van richtlijn 95/46, zoals omschreven in artikel 1, lid 1, ervan. Vervolgens heeft het Hof vastgesteld dat een systeem van verwerking van persoonsgegevens in overeenstemming is met het Unierecht indien het uitsluitend de gegevens bevat die noodzakelijk zijn voor de uitvoering van die wetgeving door deze autoriteiten, en indien door de centrale verwerking van de gegevens de uitvoering van deze wetgeving met betrekking tot het verblijfsrecht van burgers van de Unie die niet de nationaliteit van die lidstaat bezitten, efficiënter kan verlopen.

In geen geval kunnen als noodzakelijk in de zin van artikel 7, onder e), van richtlijn 95/46 worden beschouwd de bewaring en de verwerking van persoonsgegevens op naam in het kader van een dergelijk register voor statistiekdoeleinden (punten 52, 66 en 68).

Bovendien heeft het Hof er met betrekking tot de kwestie van het gebruik van de gegevens in het register voor de bestrijding van criminaliteit met name op gewezen dat dit doel ziet op de vervolging van gepleegde misdrijven en delicten, ongeacht de nationaliteit van de daders. Voor een lidstaat mag derhalve de situatie van zijn burgers, uit het oogpunt van het doel van criminaliteitsbestrijding, niet anders zijn dan die van op zijn grondgebied verblijvende burgers van de Unie die niet de nationaliteit van die lidstaat bezitten. Bijgevolg is het verschil in behandeling tussen deze burgers van de lidstaat en die burgers van de Unie dat wordt teweeggebracht door de systematische verwerking van persoonsgegevens uitsluitend betreffende burgers van de Unie die niet de nationaliteit van de betrokken lidstaat bezitten, met criminaliteitsbestrijding als doel, bij artikel 12, lid 1, EG verboden discriminatie (punten 78-80).

Arrest van 24 november 2011, ASNEF en FECEMD (C-468/10 en C-469/10, EU:C:2011:777)

De Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) en de Federación de Comercio Electrónico y Marketing Directo (FECEMD) hadden elk bij de Tribunal Supremo (hoogste rechterlijke instantie, Spanje) bestuursrechtelijk beroep ingesteld tegen een aantal artikelen van koninklijk besluit 1720/2007 waarbij uitvoering werd gegeven aan organieke wet 15/1999 tot omzetting van richtlijn 95/46.

De ASNEF en de FECEMD waren in het bijzonder van mening dat het Spaanse recht voor het verwerken van gegevens zonder toestemming van de betrokkene een voorwaarde toevoegde die in richtlijn 95/46 niet werd gesteld, op grond waarvan de gegevens moeten zijn opgenomen in „voor het publiek toegankelijke bronnen", zoals deze zijn opgesomd in artikel 3, onder j), van organieke wet 15/1999. In dit verband voerden zij aan dat deze wet en koninklijk besluit 1720/2007 de reikwijdte beperkten van artikel 7, onder f), van richtlijn 95/46, dat voor de verwerking van persoonsgegevens zonder toestemming van de betrokkene een voorwaarde stelt die uitsluitend verband houdt met het gerechtvaardigde belang van de voor de verwerking verantwoordelijke of van de derde(n) aan wie de gegevens worden verstrekt.

In dit verband heeft het Hof om te beginnen vastgesteld dat artikel 7 van richtlijn 95/46 een uitputtende lijst bevat van gevallen waarin een verwerking van persoonsgegevens zonder toestemming van de betrokkene, als rechtmatig kan worden aangemerkt. De lidstaten mogen bijgevolg niet uit hoofde van artikel 5 van die richtlijn andere beginselen betreffende de toelaatbaarheid van de verwerking van persoonsgegevens invoeren dan die welke zijn genoemd in artikel 7, noch middels bijkomende vereisten de reikwijdte van de in artikel 7 geformuleerde beginselen wijzigen. Artikel 5 staat de lidstaten immers enkel toe om, binnen de grenzen van hoofdstuk II van die richtlijn en dus binnen de grenzen van artikel 7 ervan, de voorwaarden nader te bepalen waaronder de verwerking van persoonsgegevens rechtmatig is (punten 30, 32 en 33).

In het bijzonder kunnen de lidstaten richtsnoeren opstellen voor het maken van de door artikel 7, onder f), van die richtlijn vereiste afweging van de aan de orde zijnde tegengestelde rechten en belangen. Tevens kunnen zij er rekening mee houden dat de ernst van de aantasting door die verwerking van de grondrechten van de betrokkene kan verschillen naargelang van de vraag of de desbetreffende gegevens reeds in voor het publiek toegankelijke bronnen zijn opgenomen (punten 44 en 46).

Evenwel heeft het Hof geoordeeld dat wanneer een nationale wettelijke regeling voor bepaalde categorieën persoonsgegevens de mogelijkheid van verwerking uitsluit, door voor die categorieën de uitkomst van de afweging van tegengestelde rechten en belangen definitief vast te stellen, zonder ruimte te bieden voor een afwijkende uitkomst wegens de bijzondere omstandigheden van een concreet geval, er geen sprake meer is van een nadere bepaling in de zin van artikel 5 van richtlijn 95/46. Bijgevolg kwam het Hof tot de slotsom dat artikel 7, onder f), van richtlijn 95/46 zich ertegen verzet dat een lidstaat voor bepaalde categorieën persoonsgegevens categorisch en generiek de mogelijkheid van verwerking uitsluit, zonder ruimte te bieden voor een afweging van de betrokken tegengestelde rechten en belangen in een concreet geval (punten 47 en 48).

Arrest van 19 oktober 2016, Breyer (C-582/14, EU:C:2016:779)

In dit arrest (zie tevens rubriek II.2, met het opschrift „Begrip ‚persoonsgegevens'") heeft het Hof zich tevens uitgesproken over de vraag of artikel 7, onder f), van richtlijn 95/46 zich verzet tegen een regel van nationaal recht op grond waarvan de aanbieder van onlinemediadiensten persoonsgegevens van een gebruiker zonder diens toestemming enkel mag verzamelen en benutten voor zover dit nodig is om het concrete gebruik van het onlinemedium door de betrokken gebruiker mogelijk te maken en te factureren en op grond waarvan de doelstelling, die erin bestaat de goede werking van het onlinemedium in het algemeen te waarborgen, niet rechtvaardigt dat de gegevens worden benut na afloop van de desbetreffende sessie.

Het Hof heeft geoordeeld dat artikel 7, onder f), van richtlijn 95/46 zich verzet tegen de betrokken regeling. Krachtens deze bepaling is de verwerking van persoonsgegevens in de zin van die bepaling immers rechtmatig indien de verwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de voor de verwerking verantwoordelijke of van de derde(n) aan wie de gegevens worden verstrekt, mits het belang of de fundamentele rechten en vrijheden van de betrokkene niet prevaleren. In casu had de Duitse regeling voor bepaalde categorieën persoonsgegevens categorisch en generiek de mogelijkheid van verwerking uitgesloten, zonder ruimte te bieden voor een afweging van de betrokken tegengestelde rechten en belangen in een concreet geval. Daarmee had die regeling de reikwijdte van dat in artikel 7, onder f), van richtlijn 95/46 geformuleerde beginsel op onrechtmatige wijze beperkt doordat zij eraan in de weg stond dat de doelstelling om de goede werking van het desbetreffende onlinemedium in het algemeen te waarborgen werd afgewogen tegen het belang of de fundamentele rechten en vrijheden van die gebruikers (punten 62-64 en dictum 2).

Arrest van 4 mei 2017, Rīgas satiksme (C-13/16, EU:C:2017:336)

Deze zaak was gerezen in het kader van een geschil tussen de Letse rijkspolitie en Rīgas satiksme, een trolleybusbedrijf van de stad Riga, over een verzoek om mededeling van de identificatiegegevens van de persoon die een ongeval had veroorzaakt. In deze zaak had een taxichauffeur, nadat er een verkeersongeval was gebeurd, zijn voertuig aan de rand van de weg geparkeerd. Toen de trolleybus van Rīgas satiksme langs de taxi reed, opende de passagier die op de achterbank van die taxi zat, het portier waardoor de trolleybus werd geraakt en schade opliep. Om de gang naar de civiele rechter te kunnen maken, had Rīgas satiksme onder meer de rijkspolitie verzocht om mededeling van identificatiegegevens van de persoon die het ongeval had veroorzaakt. De politie weigerde het identificatienummer en het adres van de passagier en de documenten met de verklaringen van de bij het ongeval betrokken personen te verstrekken, omdat de documenten betreffende een bestuurlijke procedure die tot sancties leidt, alleen konden worden meegedeeld aan de partijen in die zaak en, wat het identificatienummer en het adres betreft, de wet inzake de bescherming van de gegevens van natuurlijke personen de openbaarmaking van dergelijke informatie betreffende particulieren verbood.

Daarop heeft de Augstākās tiesas Administratīvo lietu departaments (hoogste rechterlijke instantie, afdeling bestuursrechtspraak, Letland) besloten het Hof de vraag voor te leggen of artikel 7, onder f), van richtlijn 95/46 de verplichting oplegt om persoonsgegevens aan een derde te verstrekken om hem in staat te stellen bij een civiele rechter een vordering tot schadevergoeding in te stellen voor schade die is veroorzaakt door de persoon op wie de

gegevensbescherming betrekking heeft en of het feit dat deze persoon minderjarig is, invloed kan hebben op de uitlegging van deze bepaling.

Het Hof heeft geoordeeld dat artikel 7, onder f), van richtlijn 95/46 aldus moet worden uitgelegd dat daarbij niet de verplichting wordt opgelegd om persoonsgegevens aan een derde te verstrekken om hem in staat te stellen bij een civiele rechter een vordering tot schadevergoeding in te stellen voor schade die is veroorzaakt door de persoon op wie de gegevensbescherming betrekking heeft. Die bepaling zou zich evenwel niet tegen een dergelijke mededeling verzetten indien deze geschiedt op basis van het nationale recht, met inachtneming van de in deze bepaling gestelde voorwaarden (punten 27, 34 en dictum).

In deze context heeft het Hof vastgesteld dat het in omstandigheden als die in het hoofdgeding, onder voorbehoud van het onderzoek dat de nationale rechter dienaangaande dient te verrichten, niet gerechtvaardigd is om te weigeren aan een benadeelde partij persoonsgegevens mee te delen die noodzakelijk zijn voor het instellen van een vordering tot schadevergoeding tegen de schadeverwekker of, in voorkomend geval, tegen de personen die het ouderlijk gezag uitoefenen, omdat de schadeverwekker minderjarig is (punt 33).

Arrest van 27 september 2017, Puškár (C-73/16, EU:C:2017:725)

In het hoofdgeding had Puškár beroep ingesteld bij de Najvyšší súd Slovenskej republiky (hoogste rechterlijke instantie van de Slowaakse Republiek) ertoe strekkende dat aan de Finančné riaditel'stvo (directie financiën), aan alle daaronder vallende belastingkantoren en aan de Kriminálny úrad finančnej správy (bureau voor bestrijding van financieel-economische criminaliteit) werd gelast zijn naam niet op te nemen op de lijst van personen die door de directie financiën worden beschouwd als stromannen. Die lijst is door deze laatste opgesteld in het kader van de belastingheffing en wordt bijgehouden door de directie financiën en door het bureau voor bestrijding van financieel-economische criminaliteit (hierna: „litigieuze lijst"). Voorts verzocht hij dat iedere hem betreffende vermelding van die lijst en van het informatiesysteem van de belastingadministratie zou worden verwijderd.

In die omstandigheden heeft de Najvyšší súd Slovenskej republiky zich tot het Hof gewend, met name met de vraag of het recht op eerbiediging van het privéleven, het familie- en gezinsleven, de woning en de communicatie, neergelegd in artikel 7 van het Handvest, en het recht op bescherming van persoonsgegevens, neergelegd in artikel 8 ervan, aldus konden worden uitgelegd dat een lidstaat niet zonder instemming van de betrokkene lijsten van persoonsgegevens ten behoeve van de belastingheffing mag aanhouden en dat dus de verkrijging van persoonsgegevens door een overheidsorgaan ten behoeve van de bestrijding van belastingfraude op zich een risico zou vormen.

Het Hof kwam tot de slotsom dat artikel 7, onder e), van richtlijn 95/46 niet eraan in de weg staat dat door de instanties van een lidstaat ten behoeve van de belastingheffing en de bestrijding van belastingfraude zonder de instemming van de betrokken personen persoonsgegevens worden verwerkt zoals het geval is met de opstelling van een lijst van personen zoals die welke aan de orde is in het hoofdgeding, mits, in de eerste plaats, aan die instanties door de nationale wetgeving taken van algemeen belang in de zin van die bepaling zijn opgedragen, de opstelling van die lijst en de inschrijving daarop van de namen van de betrokken personen daadwerkelijk

passend en noodzakelijk zijn voor de verwezenlijking van de nagestreefde doelstellingen en er voldoende aanwijzingen bestaan om te vermoeden dat de betrokken personen terecht op die lijst staan, en, in de tweede plaats, aan alle door richtlijn 95/46 opgelegde voorwaarden voor geoorloofdheid van die verwerking van persoonsgegevens is voldaan (punt 117 en dictum 3).

In dit verband heeft het Hof vastgesteld dat het aan de verwijzende rechterlijke instantie is om na te gaan of de vaststelling van de litigieuze lijst noodzakelijk is voor de uitvoering van de in het hoofdgeding aan de orde zijnde taken van algemeen belang, waarbij onder meer in aanmerking moet worden genomen wat de precieze doelstelling is van de vaststelling van de litigieuze lijst, welke rechtsgevolgen de op die lijst vermelde personen ondervinden en of die lijst al dan niet een openbare lijst is. Bovendien dient de verwijzende rechter in het licht van het evenredigheidsbeginsel na te gaan of met de vaststelling van de litigieuze lijst en de inschrijving daarop van de namen van de betrokken personen de daarmee nagestreefde doelstellingen worden bereikt en of voor de bereiking van die doelstellingen geen andere, minder vergaande middelen kunnen worden aangewend (punten 111-113).

Voorts kan volgens het Hof het feit dat een persoon op de litigieuze lijst is ingeschreven sommige van zijn rechten aantasten. Inschrijving op die lijst zou immers zijn goede naam kunnen aantasten en nadelig kunnen zijn voor zijn betrekkingen met de belastingautoriteiten. Ook zou die inschrijving afbreuk kunnen doen aan het in artikel 48, lid 1, van het Handvest geformuleerde vermoeden van onschuld van die persoon en aan de in artikel 16 van het Handvest neergelegde vrijheid van ondernemerschap van de rechtspersonen die in verband worden gebracht met de op de litigieuze lijst ingeschreven natuurlijke personen. Bijgevolg zou een dergelijke afbreuk slechts passend zijn indien er voldoende aanwijzingen zijn om de betrokken persoon ervan te verdenken dat hij fictief een directiepost bekleedt binnen de rechtspersonen die met hem in verband worden gebracht en daarmee de belastingheffing en de bestrijding van belastingfraude ondermijnt (punt 114).

Bovendien heeft het Hof geoordeeld dat zo er redenen mochten zijn om krachtens artikel 13 van richtlijn 95/46 bepaalde van de in de artikelen 6 en 10 tot en met 12 ervan neergelegde rechten, zoals het recht op informatie van de betrokken persoon, te beperken, die beperking noodzakelijk zou moeten zijn ter vrijwaring van een in lid 1 van dat artikel 13 genoemd belang, zoals inzonderheid een belangrijk economisch en financieel belang op fiscaal gebied, en moeten berusten op wettelijke maatregelen (punt 116).

Arrest van 11 november 2020, Orange Romania (C-61/19, EU:C:2020:901)

Orange România levert mobiele-telecommunicatiediensten op de Roemeense markt. Op 28 maart 2018 heeft de Autoritate Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (nationale toezichthoudende autoriteit voor de verwerking van persoonsgegevens, Roemenië) Orange România een geldboete opgelegd wegens het verzamelen en bewaren van kopieën van de identiteitsbewijzen van haar klanten zonder uitdrukkelijke toestemming van die klanten.

Volgens de ANSPDCP heeft Orange România in de periode van 1 tot en met 26 maart 2018 overeenkomsten inzake de verstrekking van telecommunicatiediensten gesloten die een clausule bevatten volgens welke de klanten in kennis zijn gesteld van en toestemming hebben gegeven voor het verzamelen en bewaren van een kopie van hun identiteitsbewijs. Het vakje

met betrekking tot deze clausule is door de verwerkingsverantwoordelijke aangevinkt vóór de ondertekening van de overeenkomst.

In deze context heeft de Tribunal București (rechter in eerste aanleg Boekarest, Roemenië) het Hof verzocht te verduidelijken onder welke voorwaarden de toestemming van de klanten voor de verwerking van persoonsgegevens geldig kan worden geacht.

Het Hof herinnert er om te beginnen aan dat het Unierecht[31] een lijst bevat van gevallen waarin een verwerking van persoonsgegevens als rechtmatig kan worden aangemerkt. In het bijzonder moet de toestemming van de betrokkene vrij, specifiek, op informatie berustend en ondubbelzinnig zijn.[32] In dit verband wordt de toestemming niet rechtsgeldig gegeven in geval van stilzwijgen, reeds aangekruiste vakjes of inactiviteit (punten 34, 36, 37 en 39).

Indien de betrokkene toestemming geeft in het kader van een schriftelijke verklaring die ook op andere aangelegenheden betrekking heeft, moet die verklaring bovendien in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal worden gepresenteerd. Om te waarborgen dat de betrokkene een echte vrije keuze heeft, mogen de contractuele bedingen hem niet misleiden omtrent de mogelijkheid om de overeenkomst te sluiten zonder in te stemmen met de verwerking van zijn gegevens (punten 34, 36, 37, 39 en 41).

Het Hof preciseert dat Orange România, aangezien zij verantwoordelijk is voor de verwerking van persoonsgegevens, moet kunnen aantonen dat de verwerking van die gegevens rechtmatig is en dus in casu dat haar klanten een geldige toestemming hebben gegeven. Aangezien de betrokken klanten het vakje betreffende het verzamelen en bewaren van kopieën van hun identiteitsbewijs niet zelf lijken te hebben aangevinkt, kan niet op grond van het enkele feit dat dit vakje is aangevinkt, worden aangetoond dat deze klanten hiermee hebben ingestemd. Het staat aan de verwijzende rechter om de daartoe vereiste controles te verrichten (punten 42 en 46).

Volgens het Hof dient deze rechter ook na te gaan of, bij gebreke van verduidelijking op dit punt, de contractuele bedingen in kwestie de klanten konden misleiden omtrent de mogelijkheid om de overeenkomst te sluiten zonder in te stemmen met de verwerking van hun gegevens. Bovendien merkt het Hof op dat Orange România van een klant die geen toestemming gaf om zijn gegevens te verwerken, eiste dat deze schriftelijk verklaarde niet in te stemmen met het verzamelen en het bewaren van de kopie van zijn identiteitsbewijs. Volgens het Hof kan een dergelijk aanvullend vereiste onnodig afbreuk doen aan de vrije keuze om zich tegen deze verzameling en bewaring te verzetten. Aangezien het hoe dan ook aan Orange România staat om aan te tonen dat haar klanten met een actieve gedraging blijk hebben gegeven van hun toestemming voor de verwerking van hun persoonsgegevens, kan zij niet van hen eisen dat zij actief blijk geven van hun weigering (punten 49-51).

Het Hof komt dan ook tot de slotsom dat een overeenkomst inzake de verstrekking van telecommunicatiediensten die een beding bevat volgens hetwelk de betrokkene in kennis is gesteld van en toestemming heeft gegeven voor het verzamelen en het bewaren van een kopie van zijn identiteitsbewijs voor identificatiedoeleinden, niet kan aantonen dat die betrokkene op

[31] Artikel 7 van richtlijn 95/46 en artikel 6 AVG.
[32] Artikel 2, onder h), van richtlijn 95/46 en artikel 4, punt 11, AVG.

geldige wijze toestemming heeft gegeven voor dat verzamelen en dat bewaren, wanneer het vakje betreffende dat beding door de voor de gegevensverwerking verantwoordelijke is aangevinkt vóór de ondertekening van die overeenkomst, wanneer de contractuele bedingen van die overeenkomst de betrokkene kunnen misleiden omtrent de mogelijkheid om de overeenkomst te sluiten zonder in te stemmen met de verwerking van zijn gegevens, of wanneer de vrije keuze om zich tegen dat verzamelen en dat bewaren te verzetten, onnodig wordt aangetast door deze verantwoordelijke doordat geëist wordt dat de betrokkene, om uiting te geven aan zijn weigering om toestemming te geven, een aanvullend formulier invult waaruit die weigering blijkt (punt 52 en dictum).

Arrest van 12 mei 2021 (Grote kamer), Bundesrepublik Deutschland (Red notice van Interpol) (C-505/19, EU:C:2021:376)

In 2012 heeft de Internationale Organisatie van Criminele Politie (hierna: „Interpol") op verzoek van de Verenigde Staten en op basis van een aanhoudingsbevel van de Amerikaanse autoriteiten een *red notice* uitgevaardigd tegen WS, Duits staatsburger, met het oog op zijn eventuele uitlevering. Wanneer een persoon ten aanzien van wie een dergelijke notice is uitgevaardigd, is gelokaliseerd in een bij Interpol aangesloten staat, dient deze staat de gezochte persoon in beginsel voorlopig aan te houden dan wel toezicht te houden op diens verplaatsingen of zijn bewegingsvrijheid te beperken.

Nog vóór de publicatie van de red notice was echter in Duitsland tegen WS een onderzoeksprocedure ingeleid die volgens de verwijzende rechter betrekking had op dezelfde feiten als die welke ten grondslag lagen aan die notice. Die procedure is in 2010 onherroepelijk beëindigd nadat WS een geldsom had betaald overeenkomstig een specifieke schikkingsprocedure waarin het Duitse strafrecht voorziet. Vervolgens heeft het Bundeskriminalamt (federale recherche, Duitsland) Interpol meegedeeld dat het van mening was dat in dit geval wegens die eerdere procedure het ne-bis-in-idembeginsel van toepassing was. Dit beginsel, dat zowel in artikel 54 van de Overeenkomst ter uitvoering van het Schengenakkoord[33] als in artikel 50 van het Handvest is verankerd, verzet zich ertegen dat een persoon die reeds bij onherroepelijk vonnis is berecht, voor hetzelfde strafbare feit opnieuw wordt vervolgd.

In 2017 heeft WS bij het Verwaltungsgericht Wiesbaden (bestuursrechter Wiesbaden, Duitsland) beroep ingesteld tegen de Bondsrepubliek Duitsland opdat deze lidstaat zou worden gelast de nodige maatregelen te nemen voor de intrekking van de hem betreffende red notice. In dit verband voert WS niet alleen aan dat het ne-bis-in-idembeginsel is geschonden, maar ook dat zijn door artikel 21 VWEU gewaarborgde recht op vrij verkeer is geschonden aangezien hij niet kan reizen naar een staat die partij is bij het Schengenakkoord of naar een lidstaat zonder het risico te lopen om te worden aangehouden. Hij is tevens van mening dat deze schendingen met zich meebrengen dat de verwerking van zijn in die red notice vervatte persoonsgegevens in

[33] Overeenkomst ter uitvoering van het te Schengen gesloten akkoord van 14 juni 1985 tussen de regeringen van de staten van de Benelux Economische Unie, de Bondsrepubliek Duitsland en de Franse Republiek betreffende de geleidelijke afschaffing van de controles aan de gemeenschappelijke grenzen (PB 2000, L 239, blz. 19) (hierna: „SUO").

strijd is met richtlijn 2016/680 betreffende de bescherming van persoonsgegevens in strafzaken[34].

Tegen deze achtergrond heeft het Verwaltungsgericht Wiesbaden besloten om het Hof vragen te stellen over de toepassing van het ne-bis-in-idembeginsel en meer bepaald over de mogelijkheid om in een situatie als die van het geding over te gaan tot de voorlopige aanhouding van een persoon ten aanzien van wie een red notice is uitgevaardigd. Bovendien wenst de verwijzende rechter, voor het geval dat dit beginsel van toepassing zou zijn, te vernemen welke gevolgen deze toepasselijkheid zou hebben voor de verwerking van de in een dergelijke notice vervatte persoonsgegevens door de lidstaten.

In het arrest van de Grote kamer oordeelt het Hof onder meer dat de bepalingen van richtlijn 2016/680, gelezen in het licht van artikel 54 SUO en artikel 50 van het Handvest, aldus moeten worden uitgelegd dat zij zich niet verzetten tegen de verwerking van persoonsgegevens die vervat zijn in een door Interpol uitgevaardigde red notice, zolang niet bij onherroepelijke rechterlijke beslissing is vastgesteld dat het ne-bis-in-idembeginsel van toepassing is op de feiten die ten grondslag liggen aan die notice, en mits die verwerking voldoet aan de in die richtlijn gestelde voorwaarden (punt 121 en dictum 2).

Wat de vraag over de in een red notice van Interpol vervatte persoonsgegevens betreft, merkt het Hof op dat elke bewerking met betrekking tot deze gegevens, zoals de vastlegging ervan in de opsporingsregisters van een lidstaat, een „verwerking" van die gegevens is die onder richtlijn 2016/680 valt.[35] Voorts oordeelt het Hof dat met deze verwerking een legitieme doelstelling wordt nagestreefd en dat die verwerking niet kan worden geacht onrechtmatig te zijn op de enkele grond dat mogelijkerwijs het ne-bis-in-idembeginsel van toepassing is op de feiten die ten grondslag liggen aan die red notice.[36] Deze verwerking door de autoriteiten van de lidstaten kan overigens juist onontbeerlijk blijken te zijn om na te gaan of dat beginsel van toepassing is (punten 111, 114, 116, 117 en 119).

Derhalve oordeelt het Hof tevens dat richtlijn 2016/680, gelezen in het licht van artikel 54 SUO en artikel 50 van het Handvest, zich niet verzet tegen de verwerking van persoonsgegevens die vervat zijn in een red notice, zolang niet bij onherroepelijke rechterlijke beslissing is vastgesteld dat het ne-bis-in-idembeginsel in het specifieke geval van toepassing is. Deze verwerking moet wel voldoen aan de in die richtlijn gestelde voorwaarden. Zij moet met name noodzakelijk zijn voor de uitvoering van een taak door een nationale bevoegde autoriteit met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen[37] (punt 121 en dictum 2).

---

34 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 (PB 2016, L 119, blz. 89).

35 Zie artikel 2, lid 1, en artikel 3, punt 2, van richtlijn 2016/680.

36 Zie artikel 4, lid 1, onder b), en artikel 8, lid 1, van richtlijn 2016/680.

37 Zie artikel 1, lid 1, en artikel 8, lid 1, van richtlijn 2016/680.

Is daarentegen het ne-bis-in-idembeginsel van toepassing, dan is de vastlegging van de in een red notice van Interpol vervatte persoonsgegevens in de opsporingsregisters van de lidstaten niet langer noodzakelijk, aangezien de betrokkene niet meer strafrechtelijk kan worden vervolgd voor de feiten waarop die notice betrekking heeft, en derhalve niet meer wegens die feiten kan worden aangehouden. Hieruit volgt dat de betrokkene moet kunnen verzoeken om wissing van zijn gegevens. Indien die vastlegging niettemin wordt gehandhaafd, moet zij gepaard gaan met de vermelding dat de betrokkene op grond van het ne-bis-in-idembeginsel voor dezelfde feiten niet meer kan worden vervolgd in een lidstaat of in een staat die partij is bij het Schengenakkoord (punt 120).

Arrest van 22 juni 2021 (Grote kamer), Latvijas Republikas Saeima (Strafpunten) (C-439/19, EU:C:2021:504)

In dit arrest (zie tevens rubriek II.3. „Begrip ‚verwerking van persoonsgegevens'") oordeelt het Hof dat de AVG in de weg staat aan de regeling die aan de Ceļu satiksmes drošības direkcija (directie verkeersveiligheid, Letland) (hierna: „CSDD") de verplichting oplegt om gegevens betreffende de strafpunten die wegens verkeersovertredingen aan bestuurders van voertuigen worden gegeven, toegankelijk te maken voor het publiek, zonder dat de persoon die om toegang verzoekt hoeft aan te tonen dat hij een specifiek belang heeft bij het verkrijgen van die gegevens. Volgens het Hof is niet aangetoond dat het – met name voor de verwezenlijking van de door de Letse regering aangehaalde doelstelling de verkeersveiligheid te verhogen – noodzakelijk is om persoonsgegevens te verstrekken die betrekking hebben op strafpunten voor verkeersovertredingen. Daarnaast is het Hof van oordeel dat noch het recht van het publiek op toegang tot officiële documenten noch het recht op vrijheid van informatie een dergelijke regeling rechtvaardigt (punten 113, 120-122 en dictum 2).

In dit verband beklemtoont het Hof dat de met de Letse regeling beoogde verhoging van de verkeersveiligheid een door de Unie erkende doelstelling van algemeen belang is, zodat de lidstaten verkeersveiligheid kunnen aanmerken als een „taak van algemeen belang"[38]. Het staat evenwel niet vast dat de Letse regeling voor het verstrekken van persoonsgegevens betreffende strafpunten noodzakelijk is voor de verwezenlijking van het nagestreefde doel. De Letse wetgever beschikt namelijk over een groot aantal actiemogelijkheden waarmee hij dat doel had kunnen bereiken door het gebruik van andere middelen, die minder inbreuk maken op de grondrechten van de betrokken personen. Daarnaast moet rekening worden gehouden met de gevoeligheid van gegevens betreffende strafpunten en met het feit dat de openbaarmaking ervan in ernstige mate inbreuk kan maken op het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens, omdat de openbaarmaking van die gegevens kan leiden tot maatschappelijke afkeuring en tot stigmatisering van de betrokken persoon (punten 109-113).

Voorts is het Hof van oordeel dat deze twee grondrechten, gelet op de gevoeligheid van de gegevens in kwestie en de ernst van de inbreuk die op deze grondrechten wordt gemaakt door de openbaarmaking van die gegevens, zowel prevaleren boven het belang dat het publiek heeft

[38] Op grond van artikel 6, lid 1, onder e), AVG is een verwerking van persoonsgegevens rechtmatig indien zij „noodzakelijk [is] voor de vervulling van een taak van algemeen belang".

bij toegang tot officiële documenten – zoals het nationale register van voertuigen en de bestuurders daarvan – als boven het recht op vrijheid van informatie (punten 120 en 121).

Bovendien oordeelt het Hof – om dezelfde redenen – dat de AVG ook in de weg staat aan de Letse regeling voor zover de CSDD daarbij wordt gemachtigd om gegevens die betrekking hebben op strafpunten die aan bestuurders van voertuigen zijn gegeven wegens verkeersovertredingen, te verstrekken aan marktdeelnemers die deze gegevens willen hergebruiken en openbaar willen maken (punt 126 en dictum 3).

Tot slot preciseert het Hof dat het beginsel van voorrang van het Unierecht zich ertegen verzet dat de verwijzende rechter de rechtsgevolgen van de naar het oordeel van het Hof met het Unierecht onverenigbare Letse regeling – waartegen bij hem beroep is ingesteld – handhaaft tot de datum waarop hij definitief uitspraak doet (punt 137 en dictum 4).

III. Verwerking van persoonsgegevens in de zin van richtlijn 2002/58

Arrest van 2 oktober 2018 (Grote kamer), Ministerio Fiscal (C-207/16, EU:C:2018:788)[39]

In deze zaak ging het om de afwijzing, door een Spaanse rechter-commissaris, van een verzoek dat was ingediend in het kader van een onderzoek inzake diefstal met geweld van een portefeuille en een mobiele telefoon. Meer in het bijzonder had de gerechtelijke politie die rechter verzocht toegang te verlenen tot de gegevens voor de identificatie van de gebruikers van de telefoonnummers die vanaf de gestolen telefoon waren geactiveerd binnen een periode van twaalf dagen vanaf de diefstal. Ter motivering van de afwijzing was aangevoerd dat de feiten die de aanleiding voor het strafrechtelijke onderzoek waren, geen „ernstig" delict vormden – dat wil zeggen, volgens het Spaanse recht, een delict dat met een gevangenisstraf van meer dan vijf jaar wordt bestraft – en dat toegang tot de identificatiegegevens immers alleen voor dat type delicten mogelijk was.

Na in herinnering te hebben gebracht dat de toegang van overheidsinstanties tot door aanbieders van elektronische-communicatiediensten bewaarde persoonsgegevens, in het kader van een strafrechtelijk onderzoek, binnen de werkingssfeer van richtlijn 2002/58 valt, heeft het Hof geoordeeld dat de toegang tot de identificatiegegevens van houders van met een gestolen mobiele telefoon geactiveerde simkaarten – zoals hun naam, voornaam en, in voorkomend geval, adres – een inmenging oplevert in de door het Handvest gewaarborgde grondrechten van laatstgenoemden op eerbiediging van het privéleven en op gegevensbescherming, zelfs al kan die inmenging om bepaalde redenen niet als „ernstig" worden aangemerkt en zonder dat van belang is of de informatie over het privéleven al dan niet gevoelig is en of de betrokkenen door die inmenging enig nadeel hebben ondervonden. Het Hof heeft echter beklemtoond dat deze inmenging niet zodanig ernstig is dat die toegang – op het gebied van het voorkomen,

[39] Dit arrest is opgenomen in het Jaarverslag 2018, blz. 92 en 93.

onderzoeken, opsporen en vervolgen van strafbare feiten – moet worden beperkt tot de bestrijding van zware criminaliteit. Hoewel richtlijn 2002/58 een uitputtende opsomming geeft van de doelstellingen die een rechtvaardiging kunnen vormen voor een nationale regeling die de toegang van overheidsinstanties tot door aanbieders van elektronische-communicatiediensten bewaarde gegevens regelt en die aldus afwijkt van het beginsel van de vertrouwelijkheid van elektronische communicatie, en deze toegang daadwerkelijk en strikt op een van die doelstellingen moet berusten, merkt het Hof immers op dat het, wat de doelstelling betreft om strafbare feiten te voorkomen, te onderzoeken, op te sporen en te vervolgen, volgens de bewoordingen van richtlijn 2002/58 bij deze doelstelling niet alleen om de bestrijding van ernstige delicten maar om „strafbare feiten" in het algemeen gaat (punten 38, 42, 59-63 en dictum).

In deze context heeft het Hof gepreciseerd dat het in het arrest *Tele2 Sverige en Watson e.a.*[40] weliswaar had geoordeeld dat alleen de bestrijding van zware criminaliteit kan rechtvaardigen dat overheidsinstanties toegang krijgen tot door aanbieders van elektronische-communicatiediensten bewaarde persoonsgegevens waaruit, in hun geheel beschouwd, precieze conclusies kunnen worden getrokken over het privéleven van de betrokken personen, doch dat die uitlegging was gemotiveerd met de overweging dat de met een toegangsregeling nagestreefde doelstelling in verhouding moet staan tot de ernst van de inmenging in de betrokken grondrechten die deze ingreep meebrengt. Volgens het evenredigheidsbeginsel kan op dat gebied een ernstige inmenging dus slechts worden gerechtvaardigd door de doelstelling om – eveneens „ernstige" – criminaliteit te bestrijden. Is de inmenging daarentegen niet ernstig, dan kan die toegang worden gerechtvaardigd door de doelstelling van het voorkomen, onderzoeken, opsporen en vervolgen van „strafbare feiten" in het algemeen (punten 54-57).

Wat het onderhavige geval betreft was het Hof van oordeel dat de toegang tot de in het betrokken verzoek bedoelde gegevens niet kon worden aangemerkt als een „ernstige" inmenging in de grondrechten van de personen op wie de gegevens betrekking hebben, omdat uit deze gegevens geen nauwkeurige conclusies over het privéleven van de betrokken personen konden worden getrokken. Het Hof is derhalve tot de slotsom gekomen dat de inmenging die door een dergelijke gegevenstoegang zou worden veroorzaakt, kan worden gerechtvaardigd door de doelstelling om „strafbare feiten" in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen, zonder dat deze strafbare feiten als „ernstig" hoeven te zijn aangemerkt (punten 61 en 62).

Arresten van 6 oktober 2020 (Grote kamer), Privacy International (C-623/17, EU:C:2020:790) en La Quadrature du Net e.a. (C-511/18, C-512/18 en C-520/18, EU:C:2020:791)[41]

De rechtspraak betreffende de bewaring van en de toegang tot persoonsgegevens op het terrein van elektronische communicatie, in het bijzonder het arrest Tele2 Sverige en Watson e.a., waarin het Hof onder meer heeft geoordeeld dat de lidstaten aanbieders van elektronische-communicatiediensten geen algemene en ongedifferentieerde verplichting tot bewaring van verkeers- en locatiegegevens kunnen opleggen, heeft geleid tot bezorgdheid bij bepaalde staten, die vrezen dat hun hierdoor een instrument is ontnomen dat zij noodzakelijk achten om de nationale veiligheid te waarborgen en criminaliteit te bestrijden.

40 Arrest Hof van 21 december 2016, *Tele2 Sverige en Watson e.a.* (C-203/15 en C-698/15, EU:C:2016:970).

41 Deze arresten zijn opgenomen in het Jaarverslag 2020, blz. 30-33.

Tegen deze achtergrond zijn bij de Investigatory Powers Tribunal (rechter die toezicht uitoefent op de onderzoeksbevoegdheden van de overheid, Verenigd Koninkrijk) (Privacy International, C-623/17), de Conseil d'État (raad van state, Frankrijk) (La Quadrature du Net e.a., gevoegde zaken C-511/18 en C-512/18) en het Grondwettelijk Hof (België) (Ordre des barreaux francophones et germanophone e.a., C-520/18) gedingen aanhangig gemaakt over de rechtmatigheid van door bepaalde lidstaten op dat terrein vastgestelde regelingen die met name voorzien in een verplichting voor aanbieders van elektronische-communicatiediensten om verkeers- en locatiegegevens van gebruikers door te zenden aan een overheidsinstantie of om deze gegevens algemeen en ongedifferentieerd te bewaren.

Bij twee arresten van 6 oktober 2020, gewezen door de Grote kamer, heeft het Hof om te beginnen geoordeeld dat nationale regelingen die aan aanbieders van elektronische-communicatiediensten een verplichting opleggen tot bewaring van verkeers- en locatiegegevens dan wel tot doorzending van deze gegevens aan de veiligheids- en inlichtingendiensten, binnen de werkingssfeer van richtlijn 2002/58 vallen (punt 49 en dictum 1 van het arrest Privacy International en punt 104 van het arrest La Quadrature du Net e.a.).

Vervolgens herinnert het Hof eraan dat richtlijn 2002/58[42] niet toelaat dat de uitzondering op de principeverplichting tot waarborging van de vertrouwelijkheid van de elektronische communicatie en van de daarmee verband houdende gegevens en op het verbod om deze gegevens op te slaan, de regel wordt. Dit betekent dat deze richtlijn de lidstaten slechts toestaat om, onder meer met het oog op de nationale veiligheid, wettelijke maatregelen te nemen ter beperking van de omvang van de in deze richtlijn bedoelde rechten en plichten, met name de verplichting om het vertrouwelijke karakter van de communicatie en van de verkeersgegevens te waarborgen[43], voor zover deze maatregelen in overeenstemming zijn met de algemene beginselen van het Unierecht, waaronder het evenredigheidsbeginsel, en met de door het Handvest gewaarborgde grondrechten[44] (punten 59 en 60 van het arrest Privacy International en punten 111 en 113 van het arrest La Quadrature du Net e.a.).

In dit verband overweegt het Hof in de zaak Privacy International dat richtlijn 2002/58, gelezen in het licht van het Handvest, zich verzet tegen een nationale regeling waarbij ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronische-communicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten wordt opgelegd. In de gevoegde zaken La Quadrature du Net e.a. en in de zaak Ordre des barreaux francophones et germanophone e.a. oordeelt het Hof dat diezelfde richtlijn zich verzet tegen wettelijke maatregelen waarbij aan aanbieders van elektronische-communicatiediensten preventief een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens wordt opgelegd.

Die verplichtingen tot doorzending en tot algemene en ongedifferentieerde bewaring van dergelijke gegevens vormen namelijk bijzonder ernstige inmengingen in de door het Handvest gewaarborgde grondrechten, zonder dat het gedrag van de personen om wier gegevens het

[42] Artikel 15, leden 1 en 3, van richtlijn 2002/58.

[43] Artikel 5, lid 1, van richtlijn 2002/58.

[44] Met name de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest.

gaat een verband vertoont met de doelstelling die door de betrokken regeling wordt nagestreefd. Op analoge wijze legt het Hof artikel 23, lid 1, AVG, gelezen in het licht van het Handvest, aldus uit dat het zich verzet tegen een nationale regeling waarbij aanbieders die het publiek online toegang verlenen tot communicatiediensten en aanbieders van opslagdiensten een verplichting tot algemene en ongedifferentieerde bewaring van met name de met die diensten verband houdende persoonsgegevens wordt opgelegd (punten 71, 82 en dictum 2 van het arrest Privacy International en punten 146, 168, 174, 177, 212 en dictum 1 en 3 van het arrest La Quadrature du Net e.a.).

Het Hof is daarentegen van mening dat in situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, richtlijn 2002/58, gelezen in het licht van het Handvest, zich niet ertegen verzet dat aan aanbieders van elektronische-communicatiediensten een bevel tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens wordt opgelegd. Het Hof preciseert in dit verband dat de beslissing waarbij dat bevel wordt opgelegd, voor een periode die niet langer is dan strikt noodzakelijk, effectief moet worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, teneinde na te gaan of een van die situaties zich voordoet en of de gestelde voorwaarden en geboden waarborgen in acht zijn genomen. Onder diezelfde voorwaarden verzet voornoemde richtlijn zich evenmin tegen de geautomatiseerde analyse van de gegevens, met name de verkeers- en locatiegegevens, van alle gebruikers van elektronische-communicatiemiddelen (punten 137-139, 177-179 en dictum 1 en 2 van het arrest La Quadrature du Net e.a.).

Het Hof voegt hieraan toe dat richtlijn 2002/58, gelezen in het licht van het Handvest, zich niet verzet tegen wettelijke maatregelen die voorzien in een gerichte bewaring, gedurende een periode die niet langer is dan strikt noodzakelijk, van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van categorieën betrokken personen of aan de hand van een geografisch criterium. Die richtlijn verzet zich evenmin tegen wettelijke maatregelen die voorzien in algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, mits de bewaartermijn wordt beperkt tot wat strikt noodzakelijk is, noch tegen wettelijke maatregelen die voorzien in een dergelijke bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische-communicatiemiddelen, waarvoor de lidstaten geen maximumbewaartermijn hoeven vast te stellen. Verder verzet die richtlijn zich niet tegen een wettelijke maatregel die het mogelijk maakt de spoedbewaring te gelasten van de gegevens waarover de dienstenaanbieders beschikken, wanneer zich situaties voordoen die het noodzakelijk maken om die gegevens ook na het verstrijken van de wettelijke bewaartermijnen te bewaren teneinde ernstige strafbare feiten of verstoringen van de nationale veiligheid op te helderen, zowel wanneer die feiten of verstoringen reeds zijn vastgesteld als wanneer er een redelijke verdenking bestaat dat dergelijke feiten zijn gepleegd of dat de nationale veiligheid wordt bedreigd (punten 161, 163, 168 en dictum 1 van het arrest La Quadrature du Net e.a.).

Bovendien oordeelt het Hof dat richtlijn 2002/58, gelezen in het licht van het Handvest, zich niet verzet tegen een nationale regeling die aanbieders van elektronische-communicatiediensten verplicht om met name verkeers- en locatiegegevens in real time op te vragen, wanneer die opvraging beperkt is tot personen ten aanzien van wie er een geldige reden bestaat om te vermoeden dat zij op een of andere manier betrokken zijn bij terroristische activiteiten, is onderworpen aan voorafgaande toetsing door een rechterlijke instantie of onafhankelijke

bestuurlijke autoriteit waarvan de beslissing bindend is, en ervoor wordt gezorgd dat een dergelijke opvraging in real time slechts wordt toegestaan binnen de grenzen van het strikt noodzakelijke. In urgente gevallen dient die toetsing op korte termijn plaats te vinden (punt 192 en dictum 2 van het arrest La Quadrature du Net e.a.).

Tot slot gaat het Hof in op de handhaving van de gevolgen van een nationale regeling die als onverenigbaar met het Unierecht is aangemerkt. Dienaangaande oordeelt het dat een nationale rechterlijke instantie geen bepaling van haar nationale recht mag toepassen die haar machtigt om de werking in de tijd te beperken van de door haar uit te spreken onwettigverklaring van een nationale regeling waarbij aan aanbieders van elektronische-communicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens wordt opgelegd die onverenigbaar is verklaard met richtlijn 2002/58, gelezen in het licht van het Handvest.

Om de verwijzende rechter een nuttig antwoord te verstrekken, brengt het Hof in herinnering dat de aanvaarding en de beoordeling van door middel van een met het Unierecht strijdige gegevensbewaring verkregen bewijzen in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van ernstige strafbare feiten, bij de huidige stand van het Unierecht uitsluitend een zaak van het nationale recht is. Het Hof preciseert evenwel dat de nationale strafrechter op grond van richtlijn 2002/58, uitgelegd in het licht van het doeltreffendheidsbeginsel, bewijzen die door middel van een met het Unierecht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens zijn verkregen, in het kader van een dergelijke strafrechtelijke procedure buiten beschouwing dient te laten indien de van strafbare feiten verdachte personen niet in de gelegenheid zijn om doeltreffend commentaar te leveren op die bewijzen (punten 222, 228 en dictum 4 van het arrest La Quadrature du Net e.a.).

Arrest van 2 maart 2021 (Grote kamer), Prokuratuur (Voorwaarden voor toegang tot elektronische-communicatiegegevens) (C-746/18, EU:C:2021:152)

In Estland is tegen H. K. een strafprocedure ingeleid wegens diefstal, gebruik van de bankpas van een ander en geweldpleging tegen personen die betrokken waren bij een gerechtelijke procedure. H. K. is voor deze strafbare feiten door een rechter in eerste aanleg veroordeeld tot een vrijheidsstraf van twee jaar. Deze beslissing is vervolgens in hoger beroep bevestigd. De processen-verbaal waarop de vaststelling van deze strafbare feiten berust, waren opgesteld op basis van met name persoonsgegevens die in het kader van de levering van elektronische-communicatiediensten waren gegenereerd. De Riigikohus (hoogste rechterlijke instantie, Estland) waarbij door H. K. cassatieberoep is ingesteld, heeft twijfels geuit omtrent de vraag of de voorwaarden waaronder de opsporingsdiensten toegang hadden tot deze gegevens verenigbaar zijn met het Unierecht[45].

Deze twijfels betreffen in de eerste plaats de vraag of de duur van de periode gedurende welke de opsporingsdiensten toegang hadden tot de gegevens, een criterium is aan de hand waarvan kan worden beoordeeld hoe ernstig een dergelijke toegang ingrijpt in de grondrechten van de betrokken personen. De verwijzende rechter vraagt zich af of het doel van bestrijding van

[45] Meer bepaald met artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest.

criminaliteit in het algemeen, en niet enkel de bestrijding van zware criminaliteit, een dergelijke inmenging kan rechtvaardigen wanneer deze periode zeer kort of de hoeveelheid verzamelde gegevens zeer beperkt is. In de tweede plaats heeft de verwijzende rechter er twijfels over of het Estse openbaar ministerie, gelet op de verschillende taken die daaraan door de nationale regelgeving zijn toevertrouwd, kan worden aangemerkt als een „onafhankelijke" bestuurlijke entiteit in de zin van het arrest Tele2 Sverige en Watson e.a.[46], die de met het onderzoek belaste instantie toegang kan verlenen tot de betrokken gegevens.

In zijn arrest, gewezen door de Grote kamer, oordeelt het Hof dat richtlijn 2002/58, gelezen in het licht van het Handvest, zich verzet tegen een nationale regeling die de mogelijkheid biedt om overheidsinstanties met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten toegang te verlenen tot een reeks verkeers- of locatiegegevens die informatie kunnen verschaffen over de communicaties van een gebruiker van een elektronische-communicatiemiddel of over de locatie van de door hem gebruikte eindapparatuur en waaruit precieze conclusies kunnen worden getrokken over zijn persoonlijke levenssfeer - welke toegang niet beperkt is tot procedures ter bestrijding van zware criminaliteit en ter voorkoming van ernstige bedreigingen van de openbare veiligheid. Volgens het Hof zijn de duur van de periode waarvoor toegang tot deze gegevens wordt gevraagd en de hoeveelheid of de aard van de voor een dergelijke periode beschikbare gegevens in dit opzicht niet van belang. Voorts is het Hof van oordeel dat deze richtlijn, gelezen in het licht van het Handvest, zich verzet tegen een nationale regeling die het openbaar ministerie de bevoegdheid verleent om een overheidsinstantie toegang te verlenen tot verkeers- en locatiegegevens met het oog op het voeren van een strafrechtelijk onderzoek (punten 45, 59 en dictum 1 en 2).

Wat de doelstelling van voorkoming, onderzoek, opsporing en vervolging van strafbare feiten betreft, die door de betrokken regeling wordt nagestreefd, is het Hof van oordeel dat overeenkomstig het evenredigheidsbeginsel alleen de bestrijding van zware criminaliteit en het voorkomen van ernstige bedreigingen van de openbare veiligheid een rechtvaardiging kunnen vormen voor de toegang van overheidsinstanties tot een reeks van verkeers- en locatiegegevens waaruit precieze conclusies kunnen worden getrokken over de persoonlijke levenssfeer van de betrokkenen, zonder dat andere factoren die de evenredigheid van een verzoek om toegang bepalen, zoals de duur van de periode waarvoor om toegang tot dergelijke gegevens wordt verzocht, tot gevolg kunnen hebben dat de doelstelling van voorkoming, onderzoek, opsporing en vervolging van strafbare feiten in het algemeen een dergelijke toegang rechtvaardigt (punten 33 en 35).

Met betrekking tot de bevoegdheid van het openbaar ministerie om een overheidsinstantie toegang te verlenen tot verkeers- en locatiegegevens teneinde een strafrechtelijk onderzoek te verrichten, herinnert het Hof eraan dat het aan het nationale recht staat om te bepalen onder welke voorwaarden aanbieders van elektronische-communicatiediensten de bevoegde nationale instanties toegang moeten verlenen tot de gegevens waarover zij beschikken. Om aan het evenredigheidsvereiste te voldoen, dient een dergelijke regeling evenwel duidelijke en nauwkeurige regels te bevatten die de reikwijdte en de toepassing van de betrokken maatregel vastleggen en minimumvereisten opleggen, zodat degenen van wie de persoonsgegevens aan de orde zijn, over voldoende waarborgen beschikken dat die gegevens doeltreffend worden

[46] Arrest van 21 december 2016, Tele2 Sverige en Watson e.a. (C-203/15 en C-698/15, EU:C:2016:970, punt 120).

beschermd tegen het risico van misbruik. Die regeling moet wettelijk verbindend zijn naar nationaal recht en aangeven in welke omstandigheden en onder welke materiële en procedurele voorwaarden een maatregel tot verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt (punt 48).

Om te waarborgen dat deze voorwaarden in de praktijk ten volle in acht worden genomen, is het volgens het Hof van wezenlijk belang dat de toegang van de bevoegde nationale instanties tot de bewaarde gegevens wordt onderworpen aan een voorafgaande toetsing door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit, en dat deze rechterlijke instantie of deze entiteit haar beslissing geeft op een met redenen omkleed verzoek van deze instanties dat met name wordt ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten. In naar behoren gemotiveerde urgente gevallen dient die toetsing op korte termijn plaats te vinden (punt 51).

Het Hof preciseert dat de voorafgaande toetsing onder meer vereist dat de rechterlijke instantie of de entiteit die met die toetsing is belast, over alle bevoegdheden beschikt en alle noodzakelijke waarborgen biedt om ervoor te zorgen dat de verschillende betrokken belangen en rechten met elkaar in overeenstemming worden gebracht. In het specifieke geval van een strafrechtelijk onderzoek vereist een dergelijke toetsing dat die rechterlijke instantie of entiteit in staat is een juist evenwicht te verzekeren tussen, enerzijds, de belangen die verband houden met de behoeften van het onderzoek in het kader van de bestrijding van criminaliteit, en, anderzijds, de fundamentele rechten op eerbiediging van de persoonlijke levenssfeer en op bescherming van de persoonsgegevens van de personen op wier gegevens de toegang betrekking heeft. Wanneer een dergelijke toetsing niet door een rechterlijke instantie maar door een onafhankelijke bestuurlijke entiteit wordt uitgeoefend, moet deze laatste een zodanige status hebben dat zij bij de uitoefening van haar taken objectief en onpartijdig kan handelen, en moet zij daartoe vrij zijn van elke invloed van buitenaf (punten 52 en 53).

Volgens het Hof volgt hieruit dat het vereiste van onafhankelijkheid waaraan de met de voorafgaande toetsing belaste instantie moet voldoen, impliceert dat die instantie de hoedanigheid van derde moet hebben ten opzichte van degene die om toegang tot de gegevens verzoekt, zodat eerstgenoemde die toetsing objectief, onpartijdig en zonder beïnvloeding van buitenaf kan verrichten. In het bijzonder impliceert het vereiste van onafhankelijkheid op strafrechtelijk gebied dat de instantie die belast is met die voorafgaande toetsing, ten eerste niet betrokken mag zijn bij de uitvoering van het betrokken strafrechtelijk onderzoek en, ten tweede, neutraal moet zijn ten opzichte van de partijen in de strafprocedure. Dat is niet het geval bij een openbaar ministerie dat, zoals het Estse parket, de onderzoeksprocedure leidt en, in voorkomend geval, optreedt als openbaar aanklager. Hieruit volgt dat het openbaar ministerie niet in een zodanige positie verkeert dat het de bovengenoemde voorafgaande toetsing kan verrichten (punten 54, 55 en 57).

IV. Doorgifte van de persoonsgegevens naar derde landen

Arrest van 6 november 2003 (Grote kamer), Lindqvist (C-101/01, EU:C:2003:596)[47]

In deze zaak (zie tevens rubriek II.3, „Begrip ‚verwerking van persoonsgegevens'") wenste de verwijzende rechter in het bijzonder te vernemen of Lindqvist persoonsgegevens had doorgegeven naar derde landen in de zin van die richtlijn.

Het Hof heeft geoordeeld dat er geen sprake is van „doorgifte van gegevens naar een derde land" in de zin van artikel 25 van richtlijn 95/46 wanneer een persoon in een lidstaat persoonsgegevens plaatst op een internetpagina die is opgeslagen bij een in dezelfde of in een andere lidstaat gevestigde natuurlijke of rechtspersoon bij wie de website is ondergebracht waarop de pagina kan worden geraadpleegd, en deze persoonsgegevens aldus toegankelijk maakt voor eenieder die een internetverbinding tot stand brengt, met inbegrip van personen die zich in derde landen bevinden (punt 71 en dictum 4).

Gezien de ontwikkeling van internet ten tijde van de opstelling van richtlijn 95/46 en het ontbreken van criteria voor het gebruik van internet in hoofdstuk IV, waarin genoemd artikel 25 is opgenomen, waarmee wordt beoogd een controle door de lidstaten van de doorgiften van persoonsgegevens naar derde landen te waarborgen en waarbij deze doorgiften worden verboden wanneer die landen geen waarborgen voor een passend beschermingsniveau bieden, kan immers niet worden aangenomen dat het de bedoeling was van de gemeenschapswetgever om, vooruitlopend op latere ontwikkelingen, het begrip „doorgifte van gegevens naar een derde land" ook te laten gelden voor een dergelijk plaatsen van persoonsgegevens op een internetpagina, ook al worden die gegevens daarmee toegankelijk gemaakt voor personen uit derde landen die de technische middelen hebben om zich toegang daartoe te verschaffen (punten 63, 64 en 68).

Arrest van 6 oktober 2015 (Grote kamer), Schrems (C-362/14, EU:C:2015:650)[48]

Schrems, Oostenrijks staatsburger en gebruiker van het sociale netwerk Facebook, had bij de Data Protection Commissioner (commissaris gegevensbescherming, Ierland) een klacht ingediend, omdat Facebook Ireland de persoonsgegevens van haar gebruikers naar de Verenigde Staten doorgaf en bewaarde op servers die zich in dat land bevinden, waar zij werden verwerkt. Volgens Schrems boden het recht en de praktijk in de Verenigde Staten geen afdoende bescherming tegen surveillance, door de overheidsinstanties, op de naar dat land doorgegeven gegevens. De Data Protection Commissioner weigerde die klacht te onderzoeken, met name omdat de Commissie in beschikking 2000/520/EG[49] had vastgesteld dat de Verenigde

[47] Dit arrest is opgenomen in het Jaarverslag 2003, blz. 67.

[48] Dit arrest is opgenomen in het Jaarverslag 2015, blz. 53.

[49] Beschikking 2000/520/EG van de Commissie van 26 juli 2000 overeenkomstig richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming geboden door de veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende Vaak gestelde vragen, die door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd (PB 2000, L 215, blz. 7).

Staten in het kader van de zogenoemde „veiligehavenregeling" (in het Engels: „safe harbour")[50], een passend beschermingsniveau waarborgden voor de doorgifte van persoonsgegevens.

In deze context heeft de High Court (rechter in eerste aanleg, Ierland) zich tot het Hof gewend met een verzoek om uitlegging van artikel 25, lid 6, van richtlijn 95/46, op grond waarvan de Commissie kan constateren dat een derde land waarborgen voor een passend beschermingsniveau voor de doorgegeven gegevens biedt, alsmede, in wezen, met een verzoek dat werd vastgesteld of beschikking 2000/520, die door de Commissie was vastgesteld op grondslag van genoemd artikel 25, lid 6, van richtlijn 95/46, geldig was.

Het Hof heeft de beschikking van de Commissie in haar geheel ongeldig verklaard en daarbij beklemtoond, allereerst, dat voor de vaststelling ervan vereist was dat naar behoren met redenen omkleed door de Commissie werd vastgesteld dat het derde land in kwestie daadwerkelijk waarborgen biedt voor een niveau van bescherming van de grondrechten dat in grote lijnen overeenkomt met dat binnen de rechtsorde van de Unie. Daar de Commissie dit in beschikking 2000/520 niet heeft vermeld, neemt artikel 1 van deze beschikking de vereisten van artikel 25, lid 6, van richtlijn 95/46, gelezen in het licht van het Handvest, niet in acht, zodat dit ongeldig is. De veiligehavenbeginselen zijn immers uitsluitend van toepassing op zelfgecertificeerde Amerikaanse organisaties die persoonsgegevens uit de Unie ontvangen, zonder dat wordt vereist dat de Amerikaanse overheidsinstanties tot naleving van die beginselen worden verplicht. Bovendien maakt beschikking 2000/520 het mogelijk dat een inmenging plaatsvindt in de grondrechten van de personen van wie de persoonsgegevens vanuit de Unie naar de Verenigde Staten zijn of zouden kunnen worden doorgegeven, zonder dat enige vaststelling is gedaan ten aanzien van de vraag of er in de Verenigde Staten overheidsregels bestaan ter beperking van dergelijke inmengingen in die rechten en zonder dat iets is vermeld over de vraag of er effectieve rechtsbescherming tegen dat soort inmengingen bestaat (punten 82, 87-89, 96-98 en dictum 2).

Voorts heeft het Hof artikel 3 van beschikking 2000/520 ongeldig verklaard voor zover daarmee aan de nationale toezichthoudende autoriteiten de bevoegdheden worden ontnomen die zij aan artikel 28 van richtlijn 95/46 ontlenen, wanneer een persoon gegevens aanvoert die twijfel kunnen doen ontstaan over de verenigbaarheid met de bescherming van het privéleven en de grondrechten en fundamentele vrijheden van personen, van een beschikking van de Commissie waarbij is geconstateerd dat een derde land waarborgen voor een passend beschermingsniveau biedt (punten 102-104). Het Hof kwam tot de slotsom dat de ongeldigheid van de artikelen 1 en 3 van beschikking 2000/520 tot gevolg had dat de geldigheid van deze beschikking in haar geheel werd aangetast (punten 105 en 106).

Met betrekking tot het feit dat een dergelijke inmenging niet kan worden gerechtvaardigd heeft het Hof om te beginnen opgemerkt dat een regeling van de Unie die een inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten met zich brengt, duidelijke en precieze regels betreffende de draagwijdte en de toepassing van een maatregel moet bevatten en minimale vereisten moet opleggen, zodat de personen van wie de persoonsgegevens aan de orde zijn, over voldoende garanties beschikken dat hun gegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk

[50] De veiligehavenregeling omvat een reeks beginselen inzake de bescherming van persoonsgegeven, die de Amerikaanse bedrijven op vrijwillige basis kunnen naleven.

onrechtmatig gebruik van deze gegevens. De noodzaak om over dergelijke garanties te beschikken is des te groter wanneer de persoonsgegevens automatisch worden verwerkt en er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd (punt 91).

Voorts, en bovenal, vereist de bescherming van het grondrecht op eerbiediging van het privéleven op het niveau van de Unie dat de uitzonderingen op de bescherming van persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven (punt 92). Niet beperkt tot het strikt noodzakelijke is dan ook een regeling die algemeen toestaat dat alle persoonsgegevens van alle personen van wie de gegevens vanuit de Unie worden doorgegeven, worden bewaard, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het nagestreefde doel en zonder dat wordt voorzien in een objectief criterium ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan voor specifieke doeleinden, die strikt beperkt zijn en als rechtvaardiging kunnen dienen voor de inmenging als gevolg van zowel de toegang tot als het gebruik van deze gegevens (punt 93). Meer bepaald vormt een regeling op grond waarvan de autoriteiten veralgemeend toegang kunnen krijgen tot de inhoud van elektronische communicatie, een aantasting van de wezenlijke inhoud van het grondrecht op eerbiediging van het privéleven. Evenzeer eerbiedigt een regeling die niet in enige beroepsmogelijkheid voor de justitiabele voorziet om toegang tot de hem betreffende persoonsgegevens te verkrijgen, of rectificatie of verwijdering van die gegevens, niet de wezenlijke inhoud van het grondrecht op een effectieve voorziening in rechte, zoals neergelegd in artikel 47 van het Handvest (punten 94 en 95).

Advies 1/15 (PNR-overeenkomst EU-Canada) van 26 juli 2017 (Grote kamer) (EU:C:2017:592)

Op 26 juli 2017 heeft het Hof zich voor het eerst uitgesproken over de verenigbaarheid van een ontwerp voor een internationale overeenkomst met het Handvest van de grondrechten van de Europese Unie, en in het bijzonder met de bepalingen inzake de eerbiediging van het privéleven en de bescherming van persoonsgegevens.

De Europese Unie en Canada hadden onderhandelingen gevoerd over een overeenkomst inzake de doorgifte en verwerking van gegevens uit het Passenger Name Record (PNR-overeenkomst); die overeenkomst is in 2014 ondertekend. Nadat de Raad van de Europese Unie het Europees Parlement om goedkeuring ervan had verzocht, heeft laatstgenoemde besloten het advies van het Hof in te winnen om te vernemen of de voorgenomen overeenkomst in overeenstemming was met het Unierecht.

De voorgenomen overeenkomst maakt de stelselmatige en continue doorgifte mogelijk van de PNR-gegevens van alle vliegtuigpassagiers aan een Canadese autoriteit met het oog op het gebruik en de bewaring ervan alsmede de eventuele latere doorgifte ervan aan andere autoriteiten en aan andere derde landen, met het doel terrorisme en zware grensoverschrijdende criminaliteit te bestrijden. Daartoe voorziet de voorgenomen overeenkomst onder meer in een periode van vijf jaar voor het bewaren van de gegevens en stelt die overeenkomst bijzondere vereisten op het gebied van de beveiliging en de integriteit van PNR-gegevens, zoals een onmiddellijke afscherming van gevoelige gegevens, en voorziet zij

ook in rechten op toegang tot de gegevens, op rectificatie en op het wissen ervan alsmede in de mogelijkheid om een bestuurlijk beroep en een beroep in rechte in te stellen.

De in de voorgenomen overeenkomst bedoelde PNR-gegevens omvatten naast, met name, de naam en de contactgegevens van de vliegtuigpassagier(s), de informatie die nodig is voor de boeking, zoals de geplande reisdata en de reisroute, informatie over de tickets, de groepen van personen die onder hetzelfde boekingsnummer geregistreerd zijn, informatie over de betaalmiddelen of de facturering, informatie over de bagage en algemene opmerkingen over de passagiers.

In zijn advies heeft het Hof geoordeeld dat de PNR-overeenkomst, wegens onverenigbaarheid van verschillende bepalingen met de door de Unie erkende grondrechten, niet kon worden gesloten in de huidige vorm ervan.

Het Hof heeft vastgesteld, in de eerste plaats, dat zowel de doorgifte van PNR-gegevens vanuit de Unie naar de bevoegde Canadese autoriteit als de door de Unie met Canada overeengekomen afbakening van de voorwaarden inzake de bewaring en het gebruik van deze gegevens en de eventuele latere doorgifte ervan aan andere Canadese autoriteiten, Europol, Eurojust, justitiële of politiële autoriteiten van de lidstaten of autoriteiten van andere derde landen een inmenging in het door artikel 7 van het Handvest gewaarborgde recht vormt. Deze handelingen vormen tevens een inmenging in het door artikel 8 van het Handvest gewaarborgde grondrecht op bescherming van persoonsgegevens, aangezien zij verwerkingen van persoonsgegevens zijn (punten 125 en 126).

Bovendien heeft het Hof beklemtoond dat bepaalde PNR-gegevens op zichzelf beschouwd weliswaar geen belangrijke informatie lijken te kunnen verschaffen over het privéleven van de betrokkenen, maar dat zij samen beschouwd onder meer een volledige reisroute kunnen blootleggen, inzicht kunnen geven in reisgewoontes en relaties tussen twee of meer personen, inlichtingen kunnen verschaffen over de financiële situatie van luchtreizigers, hun voedingsgewoonten of hun gezondheidstoestand, en zelfs gevoelige gegevens over deze passagiers kunnen bevatten, zoals gedefinieerd in artikel 2, onder e), van de voorgenomen overeenkomst (informatie waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige overtuiging etc. blijkt) (punt 128).

In dit verband heeft het Hof overwogen dat de betrokken inmengingen weliswaar kunnen worden gerechtvaardigd door een doelstelling van algemeen belang (verzekering van de openbare veiligheid bij de bestrijding van terroristische misdrijven en zware grensoverschrijdende criminaliteit), doch dat diverse bepalingen van de voorgenomen overeenkomst niet beperkt zijn tot het strikt noodzakelijke en geen duidelijke en nauwkeurige regels bevatten.

In het bijzonder heeft het Hof erop gewezen dat, rekening gehouden met het risico van een verwerking in strijd met het discriminatieverbod, voor de doorgifte van gevoelige gegevens naar Canada een nauwkeurige en bijzonder goed onderbouwde rechtvaardiging nodig is die is gebaseerd op andere gronden dan de bescherming van de openbare veiligheid tegen terrorisme en ernstige grensoverschrijdende criminaliteit. In casu ontbreekt een dergelijke rechtvaardiging echter. Het Hof heeft daaruit afgeleid dat de bepalingen van de overeenkomst

over de doorgifte van gevoelige gegevens naar Canada en over de verwerking en de bewaring van deze gegevens onverenigbaar zijn met de grondrechten (punten 165 en 232).

In de tweede plaats heeft het Hof geoordeeld dat na het vertrek van de luchtreizigers uit Canada, de duurzame opslag van de PNR-gegevens van alle luchtreizigers, die de voorgenomen overeenkomst toelaat, niet is beperkt tot wat strikt noodzakelijk is. Wat luchtreizigers betreft voor wie bij hun aankomst in Canada en tot op het ogenblik van hun vertrek uit dat land niet is vastgesteld dat zij een gevaar vormen op het gebied van terrorisme of zware grensoverschrijdende criminaliteit, lijkt er – zodra zij vertrokken zijn – tussen hun PNR-gegevens en de doelstelling van de voorgenomen overeenkomst dus geen verband – zelfs geen indirect verband – te bestaan dat de bewaring van deze gegevens rechtvaardigt. Daarentegen is het wel toelaatbaar om de PNR-gegevens van luchtreizigers ten aanzien van wie op grond van objectieve gegevens kan worden aangenomen dat zij, zelfs na hun vertrek uit Canada, een risico kunnen opleveren in het kader van de strijd tegen terrorisme en zware grensoverschrijdende criminaliteit, langer dan hun verblijf in dat land op te slaan, zelfs voor een periode van vijf jaar (punten 205-207 en 209).

In de derde plaats heeft het Hof vastgesteld dat het in artikel 7 van het Handvest van de grondrechten van de Europese Unie verankerde grondrecht op bescherming van het privéleven inhoudt dat de betrokkene zich ervan kan vergewissen dat zijn persoonsgegevens juist en rechtmatig worden verwerkt. Om de nodige verificaties te kunnen verrichten, moet hij over het recht beschikken om inzage te verkrijgen in de hem betreffende gegevens die het voorwerp van een verwerking vormen.

In dit verband heeft het Hof beklemtoond dat, in de voorgenomen overeenkomst, het van belang is dat de luchtreizigers over de doorgifte van hun PNR-gegevens aan het betrokken derde land en het gebruik van deze gegevens worden ingelicht zodra deze mededeling geen gevaar meer kan opleveren voor de onderzoeken die door de in de voorgenomen overeenkomst bedoelde publieke autoriteiten worden gevoerd. Deze informatieverstrekking is immers noodzakelijk om de luchtreizigers de mogelijkheid te bieden tot uitoefening van hun recht om inzage te vragen in de hen betreffende PNR-gegevens en in voorkomend geval de rectificatie ervan te vragen, alsook overeenkomstig artikel 47, eerste alinea, van het Handvest een doeltreffende voorziening in rechte in te stellen.

In de gevallen waarin objectieve gegevens het gebruik van de PNR-gegevens rechtvaardigen teneinde terrorisme en zware grensoverschrijdende criminaliteit te bestrijden en er een voorafgaande goedkeuring nodig is van een rechterlijke instantie of een onafhankelijke bestuurlijke entiteit, is het noodzakelijk dat de luchtreizigers individueel worden geïnformeerd. Dit geldt ook in gevallen waarin de PNR-gegevens van de luchtreizigers worden meegedeeld aan andere overheidsinstanties of aan particulieren. Een dergelijke informatieverstrekking mag evenwel pas geschieden zodra dit geen gevaar meer kan opleveren voor de onderzoeken die worden gevoerd door de in de voorgenomen overeenkomst bedoelde publieke autoriteiten (punten 219, 220, 223 en 224).

Arrest van 16 juli 2020 (Grote kamer), Facebook Ireland en Schrems (C-311/18, EU:C:2020:559)[51]

De AVG bepaalt dat de doorgifte van persoonsgegevens aan een derde land in beginsel alleen kan plaatsvinden indien het betrokken derde land een passend niveau van bescherming van die gegevens waarborgt. Volgens deze verordening kan de Commissie vaststellen dat een derde land op grond van zijn nationale wetgeving of zijn internationale verbintenissen een adequaat beschermingsniveau waarborgt.[52] Bij ontstentenis van een adequaatheidsbesluit kan een dergelijke doorgifte slechts plaatsvinden indien de in de Unie gevestigde exporteur van persoonsgegevens passende waarborgen biedt, die met name kunnen voortvloeien uit door de Commissie vastgestelde standaardbepalingen inzake gegevensbescherming, en mits de betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken.[53] Bovendien stelt de AVG nauwkeurig vast in welke gevallen een dergelijke doorgifte bij ontstentenis van een adequaatheidsbesluit of van passende waarborgen kan plaatsvinden.[54]

Maximillian Schrems, een Oostenrijks staatsburger die in Oostenrijk woont, is sinds 2008 een gebruiker van Facebook. Net zoals het geval is voor alle andere in de Unie wonende gebruikers van Facebook, worden de persoonsgegevens van Schrems door Facebook Ireland geheel of gedeeltelijk doorgegeven naar servers van Facebook Inc., die zich op het grondgebied van de Verenigde Staten bevinden, en worden zij daar verwerkt. Schrems had een klacht ingediend bij de Ierse toezichthoudende autoriteit die er in wezen toe strekte deze doorgiften te verbieden. Hij betoogde dat het recht en de praktijk in de Verenigde Staten geen toereikende bescherming bieden tegen toegang, door overheidsinstanties, tot de aan dat land doorgegeven gegevens. Deze klacht werd afgewezen op grond dat de Commissie in beschikking 2000/520 [55] had vastgesteld dat de Verenigde Staten een passend beschermingsniveau waarborgden. Bij arrest van 6 oktober 2015 heeft het Hof, waaraan een prejudiciële vraag was voorgelegd door de High Court (rechter in eerste aanleg, Ierland), geoordeeld dat dit besluit ongeldig was (hierna: „arrest Schrems I")[56] (punten 52 en 53).

Na het arrest Schrems I en de daaropvolgende nietigverklaring, door de Ierse rechter, van het besluit tot afwijzing van de klacht van Schrems, verzocht de Ierse toezichthoudende autoriteit hem zijn klacht te herformuleren gelet op de ongeldigverklaring van beschikking 2000/520 door het Hof. In zijn geherformuleerde klacht bleef Schrems erbij dat de Verenigde Staten geen afdoende bescherming van de aan dat land doorgegeven gegevens boden. Hij vorderde dat de doorgiften van zijn persoonsgegevens vanuit de Unie aan de Verenigde Staten, die Facebook Ireland toen verrichtte op basis van de standaardbepalingen inzake gegevensbescherming in de bijlage bij besluit 2010/87/EU[57], voor de toekomst zouden worden opgeschort of verboden. Daar de toezichthoudende autoriteit van mening was dat de behandeling van de klacht van Schrems met name afhing van de geldigheid van besluit 2010/87, leidde zij bij de High Court een procedure in opdat de High Court het Hof om een prejudiciële beslissing zou verzoeken.

---

51 Dit arrest is opgenomen in het Jaarverslag 2020, blz. 27-30.

52 Artikel 45 AVG.

53 Artikel 46, lid 1 en lid 2, onder c), AVG.

54 Artikel 49 AVG.

55 Beschikking van de Commissie van 26 juli 2000 overeenkomstig richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende Vaak gestelde vragen, die door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd (PB 2000, L 215, blz. 7).

56 Arrest Hof van 6 oktober 2015, Schrems (C-362/14, EU:C:2015:650) (zie tevens PC nr. 117/15).

57 Besluit van de Commissie van 5 februari 2010 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens aan in derde landen gevestigde verwerkers krachtens richtlijn 95/46/EG van het Europees Parlement en de Raad (PB 2010, L 39, blz. 5), zoals gewijzigd bij uitvoeringsbesluit (EU) 2016/2297 van de Commissie van 16 december 2016 (PB 2016, L 344, blz. 100).

Na de inleiding van deze procedure heeft Commissie uitvoeringsbesluit (EU) 2016/1250 betreffende de gepastheid van de door het EU-VS-privacyschild geboden bescherming[58] vastgesteld (punten 54, 55 en 57).

Met zijn verzoek om een prejudiciële beslissing stelde de verwijzende rechter het Hof vragen over de toepasbaarheid van de AVP op doorgiften van persoonsgegevens die zijn gebaseerd op standaardbepalingen inzake gegevensbescherming in besluit 2010/87, over het door de AVP in het kader van een dergelijke doorgifte vereiste beschermingsniveau en over de verplichtingen die in deze context op de toezichthoudende autoriteiten rusten. Voorts wierp de High Court de vraag op of besluit 2010/87 en uitvoeringsbesluit 2016/1250 geldig zijn.

Het Hof heeft vastgesteld dat bij de toetsing van besluit 2010/87 aan het Handvest niet is gebleken van feiten of omstandigheden die de geldigheid ervan kunnen aantasten. Uitvoeringsbesluit 2016/1250 heeft het Hof daarentegen ongeldig verklaard (dictum 4 en 5).

Het Hof heeft allereerst geoordeeld dat het Unierecht, en met name de AVG, van toepassing is op de doorgifte van persoonsgegevens voor commerciële doeleinden door een in een lidstaat gevestigde marktdeelnemer aan een andere, in een derde land gevestigde marktdeelnemer, zelfs indien deze gegevens tijdens of na die doorgifte door de autoriteiten van het betrokken derde land kunnen worden verwerkt ten behoeve van de openbare veiligheid, defensie en de veiligheid van de staat. Het Hof heeft gepreciseerd dat dit type gegevensverwerking door de autoriteiten van een derde land een dergelijke doorgifte niet kan uitsluiten van de werkingssfeer van de AVG (punten 86, 88, 89 en dictum 1).

Wat het in het kader van een dergelijke doorgifte vereiste beschermingsniveau betreft, heeft het Hof geoordeeld dat de daartoe door de AVG gestelde vereisten, die betrekking hebben op passende waarborgen, afdwingbare rechten en doeltreffende rechtsmiddelen, aldus moeten worden uitgelegd dat personen wier persoonsgegevens op basis van standaardbepalingen inzake gegevensbescherming aan een derde land worden doorgegeven, een bescherming dienen te genieten die in grote lijnen overeenkomt met het beschermingsniveau dat binnen de Unie wordt gewaarborgd door die verordening, gelezen in het licht van het Handvest. In deze context heeft het Hof gepreciseerd dat bij de beoordeling van dat beschermingsniveau rekening moet worden gehouden zowel met de contractuele bepalingen die zijn overeengekomen tussen de in de Unie gevestigde gegevensexporteur en de in het betrokken derde land gevestigde ontvanger van de doorgifte, als, wat een eventuele toegang van de overheidsinstanties van dat derde land tot de doorgegeven gegevens betreft, met de relevante aspecten van het rechtsstelsel van dat derde land (punt 105 en dictum 2).

Met betrekking tot de in de context van een dergelijke doorgifte op de toezichthoudende autoriteiten rustende verplichtingen, heeft het Hof geoordeeld dat deze autoriteiten, tenzij de Commissie op geldige wijze een adequaatheidsbesluit heeft vastgesteld, er met name toe verplicht zijn om de doorgifte van persoonsgegevens naar een derde land op te schorten of te verbieden, wanneer zij, gelet op alle omstandigheden van die doorgifte, van oordeel zijn dat de standaardbepalingen inzake gegevensbescherming in dat derde land niet worden of niet kunnen worden nageleefd en dat de bescherming van de doorgegeven gegevens, zoals vereist

[58] Uitvoeringsbesluit van de Commissie van 12 juli 2016 overeenkomstig richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de gepastheid van de door het EU-VS-privacyschild geboden bescherming (PB 2016, L 207, blz. 1, met rectificatie in PB 2018, L 262, blz. 90).

door het Unierecht, niet kan worden gewaarborgd met andere middelen, indien de in de Unie gevestigde gegevensexporteur niet zelf een dergelijke doorgifte heeft opgeschort of beëindigd (punt 121 en dictum 3).

Het Hof heeft vervolgens de geldigheid van besluit 2010/87 onderzocht. Volgens het Hof wordt aan de geldigheid van dit besluit niet afgedaan door het enkele feit dat de standaardbepalingen inzake gegevensbescherming daarin – wegens het contractuele karakter ervan – niet bindend zijn voor de autoriteiten van de derde landen waarnaar persoonsgegevens kunnen worden doorgegeven. Of dat besluit geldig is hangt ervan af, zo heeft het Hof gepreciseerd, of het doeltreffende mechanismen bevat waarmee in de praktijk kan worden gewaarborgd dat het door het Unierecht vereiste beschermingsniveau wordt geëerbiedigd en dat de doorgifte van persoonsgegevens op basis van dergelijke bepalingen wordt opgeschort of verboden ingeval die bepalingen worden geschonden of onmogelijk kunnen worden nageleefd. Het Hof heeft vastgesteld dat besluit 2010/87 dergelijke mechanismen instelt. In dit verband beklemtoont het Hof met name dat dit besluit een verplichting instelt voor de gegevensexporteur en voor de ontvanger van de doorgifte om vooraf na te gaan of dat beschermingsniveau in het betrokken derde land wordt geëerbiedigd en dat dit besluit deze ontvanger verplicht om de gegevensexporteur ervan in kennis te stellen indien hij er eventueel niet toe in staat is de standaardbepalingen inzake bescherming na te leven, zodat die exporteur dan de doorgifte van gegevens moet opschorten en/of de overeenkomst met die ontvanger moet beëindigen (punten 132, 136, 137, 142, 148 en dictum 4).

Ten slotte heeft het Hof de geldigheid van besluit 2016/1250 onderzocht in het licht van de vereisten die voortvloeien uit de AVG, gelezen in het licht van de bepalingen van het Handvest ter waarborging van de eerbiediging van het privéleven en het gezins- en familieleven, de bescherming van persoonsgegevens en het recht op doeltreffende rechterlijke bescherming. In dit verband heeft het Hof opgemerkt dat dit besluit, net als beschikking 2000/520, de voorrang van de vereisten inzake de nationale veiligheid, het algemeen belang of de naleving van de Amerikaanse wetgeving op de genoemde beginselen vastlegt, waardoor het mogelijk is dat er inmenging plaatsvindt in de grondrechten van personen wier persoonsgegevens aan dit derde land worden doorgegeven. Volgens het Hof zijn de beperkingen op de bescherming van persoonsgegevens die voortvloeien uit de interne regeling van de Verenigde Staten inzake de toegang tot en het gebruik door de Amerikaanse overheidsinstanties van dergelijke gegevens die vanuit de Unie aan dat derde land worden doorgegeven, en die de Commissie in besluit 2016/1250 heeft beoordeeld, niet zodanig afgebakend dat wordt voldaan aan vereisten die in grote lijnen overeenkomen met die welke in het Unierecht worden gesteld door het evenredigheidsbeginsel, aangezien de op deze regeling gebaseerde surveillanceprogramma's niet tot het strikt noodzakelijke zijn beperkt. Op basis van de vaststellingen in dat besluit merkt het Hof op dat, voor bepaalde surveillanceprogramma's, uit die regeling op geen enkele wijze blijkt dat er beperkingen op de daarin vervatte bevoegdheid voor de uitvoering van die programma's bestaan noch dat er garanties bestaan voor in die programma's potentieel bedoelde niet-Amerikanen. Het Hof heeft daaraan toegevoegd dat die regeling weliswaar vereisten bevat die de Amerikaanse autoriteiten bij de tenuitvoerlegging van de surveillanceprogramma's moeten eerbiedigen, doch de betrokkenen geen rechten verschaft die zij voor de rechtbanken tegenover de Amerikaanse overheidsdiensten kunnen afdwingen (punten 164, 165, 180-182, 184 en 185).

Met betrekking tot het vereiste van rechterlijke bescherming heeft het Hof geoordeeld dat, anders dan de Commissie in besluit 2016/1250 meende, het in dat besluit bedoelde ombudsmanmechanisme deze personen geen rechtsmiddel verschaft bij een orgaan dat waarborgen biedt die in grote lijnen overeenkomen met die welke door het Unierecht worden vereist en waarmee zowel de onafhankelijkheid van de in dat mechanisme voorziene ombudsman als het bestaan van voorschriften op grond waarvan die ombudsman bevoegd is om bindende beslissingen te nemen ten aanzien van de Amerikaanse veiligheidsdiensten, wordt verzekerd. Om al deze redenen heeft het Hof uitvoeringsbesluit 2016/1250 ongeldig verklaard (punten 195-197, 201 en dictum 5).

V. Bescherming van persoonsgegevens op internet

1. Recht van verzet tegen de verwerking van persoonsgegevens („recht om te worden vergeten")

Arrest van 13 mei 2014 (Grote kamer), Google Spain en Google (C-131/12, EU:C:2014:317)

In dit arrest (zie tevens rubriek II.3, „Begrip ‚verwerking van persoonsgegevens'") heeft het Hof de draagwijdte van de in richtlijn 95/46 vervatte rechten van toegang en van verzet tegen de verwerking van persoonsgegevens op internet nader bepaald.

Zo heeft het Hof, toen het zich uitsprak over de vraag van de omvang van de verantwoordelijkheid van de exploitant van een zoekmachine op internet, in essentie geoordeeld dat ter naleving van de in artikel 12, onder b), en artikel 14, eerste alinea, onder a), van richtlijn 95/46 gewaarborgde rechten op toegang en verzet, en voor zover aan de in deze bepalingen gestelde voorwaarden is voldaan, die exploitant onder bepaalde voorwaarden verplicht is van de resultatenlijst die na een zoekopdracht op de naam van een persoon wordt weergegeven, de koppelingen te verwijderen naar door derden gepubliceerde webpagina's waarop informatie over deze persoon is te vinden. Het Hof heeft gepreciseerd dat een dergelijke verplichting ook kan bestaan indien deze naam of deze informatie niet vooraf of gelijktijdig van deze webpagina's is gewist en, in voorkomend geval, zelfs wanneer de publicatie ervan op deze webpagina's op zich rechtmatig is (punt 88 en dictum 3).

Bovendien was aan het Hof de vraag voorgelegd of de richtlijn de betrokkene toestaat te verzoeken dat de koppelingen naar webpagina's worden verwijderd uit een dergelijke resultatenlijst op grond dat deze persoon wenst dat de informatie daarin over hem na een bepaalde tijd wordt „vergeten". Het Hof wijst er om te beginnen op dat zelfs een aanvankelijk rechtmatige verwerking van exacte gegevens na verloop van tijd niet langer met deze richtlijn verenigbaar is omdat deze gegevens niet langer noodzakelijk zijn voor de doeleinden waarvoor zij zijn verzameld of verwerkt, met name wanneer deze gegevens gelet op deze doeleinden en gelet op de verstreken tijd ontoereikend, niet of niet meer ter zake dienend of bovenmatig zijn (punt 93). Indien dus na een verzoek van de betrokkene wordt vastgesteld de opneming van deze koppelingen in de lijst thans onverenigbaar is met de richtlijn, moeten deze informatie en koppelingen van die lijst worden gewist (punt 94). In deze context veronderstelt de vaststelling

van een recht van de betrokkene dat de informatie over hem niet meer met zijn naam wordt verbonden via een resultatenlijst, niet dat de opneming van de betrokken informatie in de resultatenlijst de betrokkene schade berokkent (punt 96 en dictum 4).

Ten slotte heeft het Hof gepreciseerd dat aangezien de betrokkene op basis van zijn door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten kan verlangen dat de betrokken informatie niet meer via de opneming ervan in een dergelijke resultatenlijst ter beschikking wordt gesteld van het grote publiek, deze rechten in beginsel voorrang krijgen niet enkel op het economische belang van de exploitant van de zoekmachine, maar ook op het belang van dit publiek om deze informatie te vinden wanneer op de naam van deze persoon wordt gezocht. Dit zal echter niet het geval zijn indien de inmenging in de grondrechten van de betrokkene wegens bijzondere redenen, zoals de rol die deze persoon in het openbare leven speelt, wordt gerechtvaardigd door het overwegende belang dat het publiek erbij heeft om, door deze opneming, toegang tot de betrokken informatie te krijgen (punt 97 en dictum 4).

2. Verwerking van persoonsgegevens en intellectuele-eigendomsrechten

Arrest van 29 januari 2008 (Grote kamer), Promusicae (C-275/06, EU:C:2008:54)[59]

Promusicae, een Spaanse vereniging zonder winstoogmerk waarvan de leden producenten en uitgevers van muzikale en audiovisuele opnamen zijn, had bij de Spaanse gerechten verzocht dat Telefónica de España SAU (handelsvennootschap die onder meer actief is als internetprovider) zou worden gelast de identiteit en het adres te verstrekken van bepaalde personen aan wie zij internettoegang verschafte en van wie het „IP-adres" en de datum en het uur waarop zij met internet verbonden zijn geweest, bekend was. Volgens Promusicae gebruikten deze personen het zogeheten „peer-to-peer"- of „p2p"-programma, dat dient voor het uitwisselen van bestanden (een gebruiksvriendelijk, onafhankelijk, decentraal en met geavanceerde zoek- en downloadfuncties uitgerust middel om de inhoud van bestanden te delen), en verleenden zij via de gedeelde map van hun personal computer toegang tot muzieknummers waarvan de exploitatierechten toebehoorden aan de leden van Promusicae. Zij had dus mededeling van deze gegevens gevorderd om tegen de betrokkenen civiele procedures te kunnen instellen.

In die omstandigheden heeft de Juzgado de lo Mercantil nº 5 de Madrid (handelsrechtbank nr. 5 Madrid, Spanje) het Hof de vraag voorgelegd of op grond van de Europese wettelijke regeling de lidstaten, ter verzekering van de doeltreffende bescherming van het auteursrecht, de verplichting moeten opleggen om persoonsgegevens in het kader van een civiele procedure mee te delen.

Volgens het Hof heeft dat verzoek om een prejudiciële beslissing de vraag opgeworpen hoe de vereisten inzake de bescherming van verschillende grondrechten, namelijk enerzijds het recht op eerbiediging van het privéleven en anderzijds het recht op bescherming van de eigendom en het recht op een doeltreffend beroep, met elkaar kunnen worden verzoend.

[59] Dit arrest is opgenomen in het Jaarverslag 2008, blz. 46.

In dit verband is het Hof tot de slotsom gekomen dat de lidstaten volgens de richtlijnen 2000/31/EG betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt („richtlijn inzake elektronische handel")[60], 2001/29/EG betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij[61], 2004/48/EG betreffende de handhaving van intellectuele-eigendomsrechten[62], en 2002/58 niet gehouden zijn, in een situatie als die van het hoofdgeding de verplichting op te leggen om ter verzekering van de doeltreffende bescherming van het auteursrecht in het kader van een civiele procedure persoonsgegevens te verstrekken. De lidstaten dienen er krachtens het Unierecht bij de omzetting van deze richtlijnen wel acht op te slaan dat zij zich baseren op een uitlegging daarvan die het mogelijk maakt een juist evenwicht tussen de verschillende door de rechtsorde van de Unie beschermde grondrechten te verzekeren. Bij de tenuitvoerlegging van de maatregelen ter omzetting van deze richtlijnen moeten de autoriteiten en de rechterlijke instanties van de lidstaten vervolgens niet alleen hun nationale recht conform deze richtlijnen uitleggen, maar er ook acht op slaan dat zij zich niet baseren op een uitlegging van deze richtlijnen die in conflict zou komen met deze grondrechten of de andere algemene beginselen van het Unierecht, zoals het evenredigheidsbeginsel (punt 70 en dictum).

Arrest van 24 november 2011, Scarlet Extended (C-70/10, EU:C:2011:771)[63]

De Belgische vereniging van auteurs, componisten en uitgevers CVBA (SABAM) had geconstateerd dat internetgebruikers die van de diensten van Scarlet Extended NV, een internetprovider (hierna: „Scarlet"), gebruikmaakten, zonder toestemming en zonder rechten te betalen werken uit haar catalogus van het internet downloaden via „peer-to-peer"-netwerken. SABAM had zich tot de nationale rechter gewend en in eerste aanleg verkregen dat jegens Scarlet een bevel werd uitgevaardigd tot beëindiging van de inbreuken op het auteursrecht door het onmogelijk te maken dat haar klanten via „peer-to-peer"-programma's elektronische bestanden ontvangen of verzenden die muziekwerken uit het repertoire van SABAM bevatten.

Nadat Scarlet daar hoger beroep had ingesteld, schorste het Hof van Beroep te Brussel (België) de behandeling van de zaak teneinde het Hof om een prejudiciële beslissing te verzoeken over de vraag of een dergelijk bevel verenigbaar was met het Europese recht.

Het Hof heeft geoordeeld dat de richtlijnen 95/46, 2000/31, 2001/29, 2002/58 en 2004/48, samen gelezen en uitgelegd tegen de achtergrond van de vereisten die voortvloeien uit de bescherming van de toepasselijke grondrechten, aldus moeten worden uitgelegd dat zij eraan in de weg staan dat Scarlet door de rechter wordt gelast een filtersysteem voor alle elektronische communicatie via haar diensten in te voeren, met name door het gebruik van „peer-to-peer"-programma's, dat zonder onderscheid op al haar klanten wordt toegepast, preventief werkt, uitsluitend door haar wordt bekostigd en geen beperking in de tijd kent, en dat in staat is om op het netwerk van deze provider het verkeer van elektronische bestanden die een muzikaal,

60 Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt („Richtlijn inzake elektronische handel") (PB 2000, L 178, blz. 1).

61 Richtlijn 2001/29/EG van het Europees Parlement en de Raad van 22 mei 2001 betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij (PB 2001, L 167, blz. 10).

62 Richtlijn 2004/48/EG van het Europees Parlement en de Raad van 29 april 2004 betreffende de handhaving van intellectuele-eigendomsrechten (PB 2004, L 157, blz. 45, met rectificatie in PB 2004, L 195, blz. 16).

63 Dit arrest is opgenomen in het Jaarverslag 2011, blz. 37.

cinematografisch of audiovisueel werk bevatten waarop de verzoeker intellectuele-eigendomsrechten zou hebben, te identificeren, om de overbrenging van bestanden waarvan de uitwisseling het auteursrecht schendt, te blokkeren (punt 54 en dictum).

Volgens het Hof eerbiedigt een dergelijk bevel niet het verbod in artikel 15, lid 1, van richtlijn 2000/31 om aan een dergelijke dienstverlener een algemene verplichting van toezicht op te leggen, en evenmin het vereiste dat een juist evenwicht wordt verzekerd tussen, enerzijds, het intellectuele-eigendomsrecht en, anderzijds, de vrijheid van ondernemerschap en het recht op bescherming van persoonsgegevens en de vrijheid om informatie te ontvangen of te verstrekken (punten 40 en 49).

In deze context heeft het Hof erop gewezen dat, ten eerste, het rechterlijk bevel tot invoering van het litigieuze filtersysteem een systematische analyse van alle inhoud veronderstelt en de verzameling en identificatie van de IP-adressen van de gebruikers die illegale inhoud via het netwerk versturen. Aangezien die IP-adressen de precieze identificatie van die gebruikers mogelijk maken, vormen zij beschermde persoonsgegevens (punt 51). Ten tweede kan dat rechterlijk bevel ook de vrijheid van informatie beperken, aangezien het filtersysteem mogelijk onvoldoende onderscheid maakt tussen legale en illegale inhoud, zodat de toepassing ervan zou kunnen leiden tot de blokkering van communicatie met legale inhoud. Het wordt immers niet betwist dat de beantwoording van de vraag of een verzending legaal is, ook afhangt van de toepassing van wettelijke uitzonderingen op het auteursrecht, die verschillen van lidstaat tot lidstaat. Bovendien kunnen sommige werken in bepaalde lidstaten tot het publieke domein behoren of kunnen ze door de betrokken auteurs gratis op het internet zijn geplaatst (punt 52).

Bijgevolg heeft het Hof vastgesteld dat de betrokken nationale rechterlijke instantie bij de uitvaardiging van een rechterlijk bevel waarbij Scarlet werd verplicht het litigieuze filtersysteem in te voeren, niet het vereiste eerbiedigde dat een juist evenwicht wordt verzekerd tussen enerzijds het intellectuele-eigendomsrecht en anderzijds de vrijheid van ondernemerschap, het recht op bescherming van persoonsgegevens en de vrijheid om informatie te ontvangen of te verstrekken (punt 53).

Arrest van 19 april 2012, Bonnier Audio e.a. (C-461/10, EU:C:2012:219)

De Högsta domstol (hoogste rechter in burgerlijke en strafzaken, Zweden) verzocht het Hof om een prejudiciële beslissing over de uitlegging van de richtlijnen 2002/58 en 2004/48, in het kader van een geding van Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB en Storyside AB (hierna: „Bonnier Audio e.a.") tegen Perfect Communication Sweden AB (hierna: „ePhone") waarin ePhone opkomt tegen een door Bonnier Audio e.a. ingediend verzoek om een bevel tot verstrekking van informatie.

In deze zaak waren Bonnier Audio e.a. uitgevers, die onder meer het exclusieve recht bezaten op het reproduceren, uitgeven en distribueren van 27 boeken in de vorm van luisterboeken. Zij waren van mening dat inbreuk was gemaakt op hun exclusieve recht doordat deze 27 boeken zonder hun toestemming voor het publiek toegankelijk waren gemaakt via een FTP-server („file transfer protocol") die de uitwisseling van bestanden en de overdracht van gegevens tussen computers via internet mogelijk maakte. Derhalve hadden zij zich tot de Zweedse gerechten gewend met een verzoek tot het gelasten van mededeling van de naam en het adres van de

gebruiker van het IP-adres dat geacht werd te zijn gebruikt om de betrokken bestanden door te geven.

In deze context heeft de Högsta domstol, waarbij cassatieberoep was ingesteld, het Hof de vraag voorgelegd of het Unierecht in de weg staat aan de toepassing van een op artikel 8 van richtlijn 2004/48 gebaseerde nationale bepaling volgens welke in een civielrechtelijke procedure een internetprovider met het oog op de identificatie van een abonnee kon worden gelast aan een auteursrechthouder of diens vertegenwoordiger informatie te verstrekken over de abonnee aan wie de internetprovider het IP-adres had toegewezen dat is gebruikt om inbreuk te maken op het auteursrecht, wanneer de verzoeker een duidelijk bewijs van de inbreuk op een bepaald auteursrecht heeft vergaard en die maatregel in overeenstemming is met het evenredigheidsbeginsel.

Het Hof heeft om te beginnen in herinnering gebracht dat artikel 8, lid 3, van richtlijn 2004/48, gelezen in samenhang met artikel 15, lid 1, van richtlijn 2002/58, zich er niet tegen verzet dat de lidstaten de verplichting opleggen, persoonsgegevens aan particulieren door te geven met het oog op de civielrechtelijke vervolging van inbreuken op het auteursrecht, maar de lidstaten evenmin ertoe verplicht, in een dergelijke verplichting te voorzien. Evenwel moeten de autoriteiten en de rechterlijke instanties van de lidstaten niet alleen hun nationale recht conform deze richtlijnen uitleggen, maar er ook acht op slaan dat zij zich niet baseren op een uitlegging ervan die in conflict zou komen met de grondrechten of de andere algemene beginselen van het Unierecht, zoals het evenredigheidsbeginsel (punten 55 en 56).

In dit verband heeft het Hof opgemerkt dat ingevolge de betrokken nationale wettelijke regeling een bevel tot mededeling van de betrokken gegevens slechts kon worden gegeven indien duidelijke bewijzen van een inbreuk op een intellectuele-eigendomsrecht op een werk zijn overgelegd, de gevraagde gegevens de opsporing van een inbreuk op het auteursrecht kunnen vergemakkelijken en het belang van de redenen voor dit bevel opweegt tegen de ongemakken of andere nadelen ervan voor degene tot het wie het is gericht, of tegen enig ander daarmee strijdig belang (punt 58).

Bijgevolg luidde de slotsom van het Hof dat de richtlijnen 2002/58 en 2004/48 niet in de weg staan aan een nationale wettelijke regeling als die in het hoofdgeding, voor zover deze regeling de nationale rechterlijke instantie waarbij door een persoon met procesbevoegdheid een verzoek om een bevel tot mededeling van persoonsgegevens is ingediend, in staat stelt om de in het geding zijnde tegengestelde belangen af te wegen op basis van de concrete omstandigheden van de zaak en daarbij terdege rekening te houden met de uit het evenredigheidsbeginsel voortvloeiende vereisten (punt 61 en dictum).

Arrest van 17 juni 2021, M.I.C.M. (C-597/19, EU:C:2021:492)

De onderneming Mircom International Content Management & Consulting (M.I.C.M.) Limited (hierna: „Mircom") heeft bij de ondernemingsrechtbank Antwerpen (België) (hierna: „verwijzende rechter") een verzoek om informatie ingediend tegen Telenet BVBA, een internetprovider. Met dit verzoek wordt beoogd een beslissing te verkrijgen waarbij Telenet wordt gelast om aan de hand van de IP-adressen die een gespecialiseerde onderneming voor Mircom heeft verzameld, de identificatiegegevens van Telenetklanten over te leggen. De internetverbindingen van

Telenetklanten zijn gebruikt om via het BitTorrentprotocol films uit de catalogus van Mircom op een peer-to-peernetwerk te delen. Telenet verzet zich tegen het verzoek van Mircom.

In deze context heeft de verwijzende rechter het Hof om te beginnen gevraagd of het delen op dit netwerk van onderdelen van een mediabestand met een beschermd werk krachtens het Unierecht een mededeling aan het publiek vormt. Voorts wenst hij te vernemen of een houder van intellectuele-eigendomsrechten, zoals Mircom, die deze rechten niet exploiteert, maar schadevergoeding vordert van vermeende inbreukmakers, gebruik kan maken van de maatregelen, procedures en rechtsmiddelen waarin het Unierecht voorziet om de eerbiediging van die rechten te verzekeren, bijvoorbeeld door om informatie te verzoeken. Ten slotte heeft de verwijzende rechter het Hof verzocht duidelijkheid te verschaffen over de vraag of Mircom de IP-adressen van de klanten op rechtmatige wijze heeft verzameld en of het rechtmatig is om de door Mircom aan Telenet gevraagde gegevens te verstrekken.

Het Hof is van oordeel dat het Unierecht[64] er in beginsel niet aan in de weg staat dat de IP-adressen van gebruikers van peer-to-peernetwerken wier internetverbindingen zouden zijn gebruikt voor inbreukmakende handelingen, systematisch door de houder van intellectuele-eigendomsrechten of door een derde voor diens rekening worden geregistreerd (verwerking van gegevens in een eerder stadium), en zich evenmin ertegen verzet dat de namen en de postadressen van deze gebruikers worden meegedeeld aan deze houder of derde ten behoeve van een schadevordering (verwerking van gegevens in een later stadium). De initiatieven en verzoeken ter zake moeten evenwel gerechtvaardigd en evenredig zijn, mogen geen misbruik vormen en moeten mogelijk zijn gemaakt door een nationale wettelijke maatregel die de reikwijdte van Unierechtelijke rechten en plichten beperkt. Het Hof verduidelijkt dat het Unierecht voor een vennootschap als Telenet geen verplichting inhoudt om persoonsgegevens aan particulieren mee te delen met het oog op de civielrechtelijke vervolging van inbreuken op het auteursrecht. Het Unierecht staat de lidstaten evenwel toe om een dergelijke verplichting op te leggen (punten 97, 125-127 en dictum 3).

3. Verwijdering van persoonsgegevens

Arrest van 24 september 2019 (Grote kamer), GC e.a. (Verwijdering van links naar gevoelige gegevens) (C-136/17, EU:C:2019:773)[65]

In dit arrest heeft het Hof (Grote kamer) nader bepaald welke verplichtingen de exploitant van een zoekmachine heeft in het kader van een verzoek tot verwijdering van links naar gevoelige gegevens.

Google had geweigerd verzoeken van vier personen in te willigen waarmee werd gevraagd om verwijdering van verschillende links naar door derden gepubliceerde webpagina's, met name persartikelen, uit de resultatenlijst die door de zoekmachine wordt weergegeven na een op hun respectieve naam verrichte zoekopdracht. Na klachten van deze vier personen weigerde de

64 Artikel 6, lid 1, onder f), AVG en artikel 15, lid 1, van richtlijn 2002/58.
65 Dit arrest is opgenomen in het Jaarverslag 2019, blz. 120-122.

Commission nationale de l'informatique et des libertés (CNIL; nationale commissie voor informatica en vrijheden, Frankrijk) Google aan te manen om de gevraagde verwijderingen uit te voeren. De Conseil d'État (raad van state, Frankrijk), waarbij de zaak aanhangig was gemaakt, verzocht het Hof nader te bepalen welke verplichtingen krachtens richtlijn 95/46 op de exploitant van een zoekmachine rusten bij de behandeling van een verzoek tot verwijdering.

In de eerste plaats heeft het Hof in herinnering gebracht dat – onder voorbehoud van bepaalde uitzonderingen en afwijkingen – de verwerking van persoonsgegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt, alsook de verwerking van gegevens die de gezondheid of het seksuele leven betreffen, verboden is.[66] Wat verwerkingen van gegevens inzake overtredingen, strafrechtelijke veroordelingen of veiligheidsmaatregelen betreft, deze mogen in beginsel alleen worden verricht onder toezicht van de overheid of indien de nationale wetgeving voorziet in passende specifieke waarborgen[67] (punten 39 en 40).

Het Hof heeft geoordeeld dat het verbod en de beperkingen inzake de verwerking van die bijzondere categorieën gegevens van toepassing zijn op de exploitant van een zoekmachine, net als op iedere andere voor de verwerking verantwoordelijke. De doelstelling van deze verboden en beperkingen bestaat immers in het waarborgen van een versterkte bescherming tegen dergelijke verwerkingen die, wegens de bijzondere gevoeligheid van deze gegevens een bijzonder ernstige inbreuk kunnen vormen op de grondrechten op eerbiediging van het privéleven en bescherming van persoonsgegevens (punten 42-44).

De exploitant van een zoekmachine is echter niet verantwoordelijk voor het feit dat persoonsgegevens op een door een derde gepubliceerde webpagina staan, maar voor het feit dat deze pagina wordt geïndexeerd. In die omstandigheden gelden het verbod op en de beperkingen inzake de verwerking van gevoelige gegevens alleen voor deze exploitant op grond van het feit dat hij deze indexering verricht, en dus bij een beoordeling, onder toezicht van de bevoegde nationale autoriteiten, naar aanleiding van een door de betrokkene ingediend verzoek (punten 46 en 47).

In de tweede plaats heeft het Hof overwogen dat de exploitant, na de ontvangst van een verzoek tot verwijdering dat betrekking heeft op gevoelige gegevens, onder voorbehoud van bepaalde uitzonderingen, in beginsel verplicht is dat verzoek in te willigen. Wat deze uitzonderingen betreft, kan de exploitant met name weigeren een dergelijk verzoek in te willigen wanneer hij vaststelt dat de links naar gegevens leiden die kennelijk door de betrokkene openbaar zijn gemaakt[68], mits de indexering van dergelijke links voldoet aan de andere voorwaarden voor rechtmatigheid van een verwerking van persoonsgegevens en tenzij de betrokkene het recht heeft zich tegen deze verwerking te verzetten om redenen die verband houden met zijn bijzondere situatie[69] (punten 65 en 69).

In ieder geval moet de exploitant van een zoekmachine na de ontvangst van een verzoek tot verwijdering van een link nagaan of de opname van de link naar een webpagina waarop gevoelige gegevens zijn gepubliceerd, op de resultatenlijst die wordt weergegeven na een

66 Artikel 8, lid 1, van richtlijn 95/46 en artikel 9, lid 1, van verordening 2016/679.
67 Artikel 8, lid 5, van richtlijn 95/46 en artikel 10 van verordening 2016/679.
68 Artikel 8, lid 2, onder e), van richtlijn 95/46 en artikel 9, lid 2, onder e), van verordening 2016/679.
69 Artikel 14, eerste alinea, onder a), van richtlijn 95/46 en artikel 21, lid 1, van verordening 2016/679.

zoekopdracht op de naam van de betrokkene, strikt noodzakelijk is ter bescherming van het recht op vrijheid van informatie van internetgebruikers die mogelijk geïnteresseerd zijn in toegang tot deze webpagina via een dergelijke zoekopdracht. In dit verband heeft het Hof beklemtoond dat de rechten op eerbiediging van het privéleven en op bescherming van persoonsgegevens weliswaar in de regel voorrang hebben op het recht op vrijheid van informatie van internetgebruikers, doch dat dit evenwicht in bijzondere gevallen kan afhangen van de aard van de betrokken informatie en de gevoeligheid ervan voor het privéleven van de betrokkene en van het belang dat het publiek erbij heeft om over deze informatie te beschikken, wat met name wordt bepaald door de rol die deze persoon in het openbare leven speelt (punten 66 en 68).

In de derde plaats heeft het Hof geoordeeld dat het in het kader van een verzoek tot verwijdering dat betrekking heeft op gegevens over een strafrechtelijke procedure tegen de betrokkene, die verband houden met een voorgaande fase van deze procedure en niet langer overeenkomen met de huidige situatie, aan de exploitant van de zoekmachine is om te beoordelen of deze persoon, gelet op alle omstandigheden van de zaak, er recht op heeft dat de desbetreffende informatie in het huidige stadium niet langer wordt verbonden aan zijn naam op een resultatenlijst die wordt weergegeven na een zoekopdracht op deze naam. Zelfs indien dat niet het geval is, omdat de opname van de betrokken link strikt noodzakelijk blijkt om de rechten op de eerbiediging van het privéleven en op de bescherming van de gegevens van de betrokkene te rijmen met de vrijheid van informatie van mogelijk geïnteresseerde internetgebruikers, dient de exploitant echter uiterlijk bij het verzoek tot verwijdering de resultatenlijst zodanig te ordenen dat het algehele beeld dat hiermee voor de internetgebruiker wordt geschetst, een afspiegeling vormt van de actuele gerechtelijke situatie, hetgeen onder meer vereist dat de links naar webpagina's die daarover informatie bevatten als eerste op deze lijst verschijnen (punten 77 en 78).

Arrest van 24 september 2019 (Grote kamer), Google (Territoriale werkingssfeer van de verwijdering van links) (C-507/17, EU:C:2019:772)[70]

De Commission nationale de l'informatique et des libertés (CNIL; nationale commissie voor informatica en vrijheden, Frankrijk) had Google aangemaand om bij het inwilligen van een verzoek tot verwijdering van links naar webpagina's met persoonsgegevens van de betrokken persoon uit de resultatenlijst die wordt weergegeven na een zoekopdracht op de naam van de betrokkene, tot deze verwijdering over te gaan voor alle domeinnaamextensies van haar zoekmachine. Na de weigering van Google om daaraan gevolg te geven, had de CNIL haar een geldboete van 100 000 EUR opgelegd. De Conseil d'État (raad van state, Frankrijk), waarbij Google beroep had ingesteld, verzocht het Hof nader te bepalen wat de territoriale werkingssfeer is van de verplichting voor de exploitant van een zoekmachine om overeenkomstig richtlijn 95/46 uitvoering te geven aan het recht op verwijdering van links.

Allereerst heeft het Hof in herinnering gebracht dat natuurlijke personen op grond van het Unierecht de mogelijkheid hebben om hun recht op verwijdering van links uit te oefenen ten aanzien van de exploitant van een zoekmachine die een of meerdere vestigingen heeft op het grondgebied van de Unie, ongeacht of de verwerking van persoonsgegevens (in casu de

[70] Dit arrest is opgenomen in het Jaarverslag 2019, blz. 122 en 123.

indexering van links naar webpagina's met daarop de persoonsgegevens van de persoon die zich op dat recht beroept) in de Unie plaatsvindt.[71]

Wat de reikwijdte van het recht op verwijdering van links betreft, heeft het Hof vastgesteld dat de exploitant van een zoekmachine niet gehouden is deze links te verwijderen voor alle versies van zijn zoekmachine doch enkel voor alle lidstaatspecifieke versies van die zoekmachine. Het Hof heeft in dit verband opgemerkt dat een universele verwijdering van de links, gelet op de kenmerken van internet en van de zoekmachines, weliswaar ten volle zou beantwoorden aan de doelstelling van de Uniewetgever, namelijk in de gehele Unie een hoog niveau van bescherming van persoonsgegevens te waarborgen, doch dat uit het Unierecht[72] geenszins blijkt dat de wetgever, teneinde dat doel te verwezenlijken, ervoor zou hebben gekozen om aan het recht op verwijdering van links een werkingssfeer toe te kennen die verder reikt dan het grondgebied van de lidstaten. Terwijl het Unierecht mechanismen instelt voor samenwerking tussen de toezichthoudende autoriteiten van de lidstaten om te komen tot een gezamenlijk besluit dat gebaseerd is op een afweging tussen het recht op eerbiediging van het privéleven en op bescherming van persoonsgegevens enerzijds en het belang van het publiek van de verschillende lidstaten om toegang te hebben tot bepaalde informatie anderzijds, zijn dergelijke instrumenten thans niet voorzien wat betreft de reikwijdte van de verwijdering van links buiten de Unie (punten 62 en 73).

Bij de huidige stand van het Unierecht dient de exploitant van een zoekmachine de gevraagde verwijdering van links niet enkel uit te voeren voor de versie van deze zoekmachine die specifiek is voor de lidstaat waar de begunstigde van de verwijdering verblijft, maar voor alle lidstaatspecifieke versies van de zoekmachine, dit, met name, om een consistent en hoog beschermingsniveau te bieden in de gehele Unie. Bovendien dient een dergelijke exploitant, indien nodig, maatregelen te nemen die voldoende doeltreffend zijn om internetgebruikers in de Unie te beletten of op zijn minst hen ernstig te ontmoedigen om toegang te krijgen, in voorkomend geval via een versie van de zoekmachine die specifiek is voor een derde land, tot de links waarop de verwijdering betrekking heeft, en het staat aan de nationale rechter om na te gaan of de door de exploitant genomen maatregelen voldoen aan dit vereiste (punt 70).

Ten slotte heeft het Hof beklemtoond dat het Unierecht de exploitant van een zoekmachine weliswaar niet verplicht om tot een verwijdering van links over te gaan voor alle versies van zijn zoekmachine, maar hem dit ook niet verbiedt. Bijgevolg is een toezichthoudende autoriteit of een rechterlijke instantie van een lidstaat nog steeds bevoegd om in het licht van de nationale maatstaven voor de bescherming van de grondrechten een afweging te maken tussen het recht van de betrokkene op eerbiediging van zijn privéleven en op bescherming van zijn persoonsgegevens enerzijds en de vrijheid van informatie anderzijds, en om na deze afweging de exploitant van de betreffende zoekmachine in voorkomend geval te gelasten de links te verwijderen voor alle versies van die zoekmachine (punten 65 en 72).

4. Toestemming van de gebruiker van een website voor de opslag van informatie

[71] Artikel 4, lid 1, onder a), van richtlijn 95/46 en artikel 3, lid 1, van verordening 2016/679.
[72] Artikel 12, onder b), en artikel 14, eerste alinea, onder a), van richtlijn 95/46 en artikel 17, lid 1, van verordening 2016/679.

Arrest van 1 oktober 2019 (Grote kamer), Planet49 (C-673/17, EU:C:2019:801)[73]

In dit arrest heeft het Hof geoordeeld dat de toestemming voor het opslaan van en de toegang tot informatie door middel van op de eindapparatuur van de gebruiker van een website geïnstalleerde cookies niet rechtsgeldig is verleend wanneer die toestemming voortvloeit uit een standaard aangevinkt selectievakje, ongeacht of het bij de betrokken informatie om persoonsgegevens gaat. Voorts heeft het Hof gepreciseerd dat de aanbieder van diensten de gebruiker van een website moet informeren over de vraag hoelang de cookies actief blijven en of derden al dan niet toegang tot die cookies kunnen hebben.

Het hoofdgeding betrof de organisatie van een reclameloterij door Planet49 op de website www.dein-macbook.de. Om deel te nemen moesten de internetgebruikers hun naam en adres invoeren op een website waarop selectievakjes stonden. Het vakje dat de installatie van cookies toestond was standaard aangevinkt. Nadat door de Duitse federale vereniging van consumentenbeschermingsorganisaties beroep was ingesteld, had het Bundesgerichtshof (hoogste federale rechter in burgerlijke en strafzaken, Duitsland) twijfels over de geldigheid van het verkrijgen van toestemming van de gebruikers middels een standaard aangevinkt vakje alsmede over de omvang van de op de aanbieder van de dienst rustende informatieplicht.

Het verzoek om een prejudiciële beslissing had hoofdzakelijk betrekking op de uitlegging van het begrip „toestemming" als bedoeld in richtlijn 2002/58[74], gelezen in samenhang met richtlijn 95/46[75] en met de AVG[76].

In de eerste plaats heeft het Hof opgemerkt dat artikel 2, onder h), van richtlijn 95/46, waarnaar artikel 2, onder f), van richtlijn 2002/58 verwijst, „toestemming" omschrijft als „elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem/haar betreffende persoonsgegevens worden verwerkt". Het Hof heeft opgemerkt dat met het vereiste van een „wilsuiting" van de betrokkene duidelijk naar een actieve en niet naar een passieve gedraging wordt verwezen. Toestemming door middel van een standaard aangevinkt selectievakje impliceert evenwel geen actieve gedraging van de gebruiker van een website. Voorts lijkt de ontstaansgeschiedenis van artikel 5, lid 3, van richtlijn 2002/58, dat sinds de wijziging ervan bij richtlijn 2009/136 bepaalt dat de gebruiker „toestemming [moet hebben] verleend" voor het plaatsen van cookies, erop te wijzen dat de toestemming van de gebruiker voortaan niet langer kan worden verondersteld en moet voortvloeien uit een actieve gedraging zijnerzijds. Ten slotte is een actieve toestemming thans voorgeschreven in de AVG.[77] Artikel 4, punt 11, daarvan vereist een wilsuiting in de vorm van, met name, een „ondubbelzinnige actieve handeling" en overweging 32 daarvan sluit uitdrukkelijk uit dat „stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit" als toestemming mogen gelden (punten 49, 52, 56 en 62).

Het Hof heeft derhalve geoordeeld dat de toestemming niet rechtsgeldig is verleend wanneer de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van de gebruiker van een website, wordt toegestaan door middel van een standaard aangevinkt selectievakje dat de gebruiker moet uitvinken ingeval hij weigert zijn

73 Dit arrest is opgenomen in het Jaarverslag 2019, blz. 123-125.

74 Artikel 2, onder f), en artikel 5, lid 3, van richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 (PB 2009, L 337, blz. 11).

75 Artikel 2, onder h), van richtlijn 95/46.

76 Artikel 6, lid 1, onder a), van verordening 2016/679.

77 Idem.

toestemming te verlenen. Het Hof heeft daaraan toegevoegd dat het feit dat een dergelijke gebruiker op de knop voor deelname aan de betrokken reclameloterij heeft geklikt, niet volstaat om aan te nemen dat hij rechtsgeldig toestemming heeft gegeven voor het plaatsen van cookies (punt 63).

In de tweede plaats heeft het Hof vastgesteld dat artikel 5, lid 3, van richtlijn 2002/58 de gebruiker beoogt te beschermen tegen inmenging in zijn privéleven, ongeacht of die inmenging betrekking heeft op persoonsgegevens. Daaruit volgt dat het begrip „toestemming" niet verschillend dient te worden uitgelegd naargelang de informatie die is opgeslagen in de eindapparatuur van de gebruiker van een website of daaruit is opgevraagd, al dan niet bestaat in persoonsgegevens (punten 69 en 71).

In de derde plaats heeft het Hof opgemerkt dat artikel 5, lid 3, van richtlijn 2002/58 vereist dat de gebruiker toestemming heeft verleend na te zijn voorzien van duidelijke en volledige informatie, onder meer over het doeleinde van de verwerking. Duidelijke en volledige informatie houdt in dat de gebruiker in staat is om gemakkelijk de gevolgen te bepalen van eventueel door hem te verlenen toestemming en dat gewaarborgd is dat hij deze toestemming met kennis van zaken verleent. In dit verband heeft het Hof overwogen dat de vragen hoelang de cookies actief blijven en of derden al of niet toegang tot deze cookies kunnen hebben, deel uitmaken van de duidelijke en volledige informatie die door de aanbieder van diensten aan de gebruiker van een website moet worden verstrekt (punten 73-75 en 81).

VI. Nationale toezichthoudende autoriteiten

1. Strekking van het vereiste van onafhankelijkheid

Arrest van 9 maart 2010 (Grote kamer), Commissie/Duitsland (C-518/07, EU:C:2010:125)[78]

Met haar verzoekschrift had de Commissie het Hof verzocht vast te stellen dat de Bondsrepubliek Duitsland de verplichtingen niet was nagekomen die op haar rustten krachtens artikel 28, lid 1, tweede alinea, van richtlijn 95/46, doordat de autoriteiten die belast zijn met het toezicht op de verwerking van persoonsgegevens in de niet-publieke sector in de verschillende deelstaten aan overheidstoezicht waren onderworpen, waardoor het vereiste van „volledige onafhankelijkheid" van de autoriteiten die belast zijn met het waarborgen van de bescherming van die gegevens, onjuist was uitgevoerd.

De Bondsrepubliek Duitsland was van mening dat artikel 28, lid 1, tweede alinea, van richtlijn 95/46 een functionele onafhankelijkheid van de toezichthoudende autoriteiten vereist, in die zin dat deze autoriteiten onafhankelijk moeten zijn ten opzichte van de organen van de niet-publieke sector waarop zij toezicht uitoefenen en niet onderhevig mogen zijn aan beïnvloeding van buitenaf. Het overheidstoezicht in de Duitse deelstaten was haars inziens geen beïnvloeding van buitenaf, maar een bestuurlijk intern mechanisme van toezicht door instanties binnen

78 Dit arrest is opgenomen in het Jaarverslag 2010, blz. 34.

hetzelfde bestuursapparaat als de toezichthoudende autoriteiten, die, evenals deze laatste autoriteiten, de doelstellingen van richtlijn 95/46 moeten vervullen.

Het Hof heeft geoordeeld dat de in richtlijn 95/46 voorziene waarborg van onafhankelijkheid van de nationale toezichthoudende autoriteiten de doeltreffendheid en de betrouwbaarheid van het toezicht op de naleving van de bepalingen inzake de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens beoogt te verzekeren en tegen de achtergrond van deze doelstelling moet worden uitgelegd. Die waarborg is niet ingevoerd om deze autoriteiten zelf en hun gemachtigden een bijzondere positie te verlenen, maar om een grotere bescherming te bieden aan de personen en organen die door hun beslissingen worden getroffen. Derhalve moeten de toezichthoudende autoriteiten bij de uitoefening van hun taken objectief en onpartijdig handelen (punt 25).

Het Hof heeft vastgesteld dat deze autoriteiten die belast zijn met het toezicht op de verwerking van persoonsgegevens in de niet-publieke sector, een onafhankelijkheid moeten genieten die hen in staat stelt om hun taken zonder beïnvloeding van buitenaf te vervullen. Deze onafhankelijkheid sluit niet enkel elke beïnvloeding door de organen waarop toezicht wordt uitgeoefend, uit, maar ook elk bevel of elke andere beïnvloeding van buitenaf, rechtstreeks of indirect, die de vervulling door deze autoriteiten van hun taak, een juist evenwicht tussen de bescherming van het recht op bescherming van de persoonlijke levenssfeer en het vrije verkeer van persoonsgegevens te vinden, in het gedrang zou kunnen brengen. Het gevaar alleen al dat de instanties die belast zijn met het overheidstoezicht, een politieke invloed kunnen uitoefenen op de beslissingen van de bevoegde toezichthoudende autoriteiten, volstaat om de onafhankelijke vervulling van hun taken te hinderen. Ten eerste zou er sprake kunnen zijn van een „geanticipeerde gehoorzaamheid" van deze autoriteiten in het licht van de beslissingspraktijk van de instantie die belast is met het overheidstoezicht. Ten tweede vereist de door deze autoriteiten vervulde rol van hoeders van het recht op bescherming van de persoonlijke levenssfeer dat de beslissingen van deze toezichthoudende autoriteiten, en dus de autoriteiten zelf, boven iedere verdenking van partijdigheid staan. Volgens het Hof is overheidstoezicht op de nationale toezichthoudende autoriteiten dus niet verenigbaar is met het vereiste van onafhankelijkheid (punten 30, 36, 37 en dictum).

Arrest van 16 oktober 2012 (Grote kamer), Commissie/Oostenrijk (C-614/10, EU:C:2012:631)

Met haar verzoekschrift verzocht de Commissie het Hof vast te stellen dat Oostenrijk, door niet alle nodige maatregelen te nemen om te verzekeren dat de in Oostenrijk geldende wettelijke regeling, wat de Datenschutzkommission (commissie gegevensbescherming) betreft, die is ingesteld als toezichthoudende autoriteit voor de bescherming van persoonsgegevens, voldeed aan het criterium van onafhankelijkheid, de krachtens artikel 28, lid 1, tweede alinea, van richtlijn 95/46 op hem rustende verplichtingen niet was nagekomen.

Het Hof stelde niet-nakoming door Oostenrijk vast, en overwoog in wezen dat de lidstaat die een regeling instelt op grond waarvan de bestuurder van die autoriteit een overheidsambtenaar is die is onderworpen aan bestuurlijk toezicht, het secretariaat ervan is geïntegreerd in de diensten van de nationale regering en de nationale regeringsleider een onvoorwaardelijk recht heeft op informatie over alle aspecten van het beheer van die autoriteit, niet voldoet aan het in richtlijn 95/46 geformuleerde criterium van onafhankelijkheid (punt 66 en dictum).

Het Hof heeft om te beginnen in herinnering gebracht dat de woorden „in volledige onafhankelijkheid" in artikel 28, lid 1, tweede alinea, van richtlijn 95/46 impliceren dat de toezichthoudende autoriteiten een onafhankelijkheid moeten genieten die hen in staat stelt om hun taken zonder beïnvloeding van buitenaf te vervullen. Dat een dergelijke autoriteit functioneel onafhankelijk is, nu haar leden bij de uitoefening van hun functie onafhankelijk zijn en door geen enkele instructie zijn gebonden, volstaat als zodanig niet om die toezichthoudende autoriteit voor elke beïnvloeding van buitenaf te behoeden. Met de in dit kader vereiste onafhankelijkheid wordt niet alleen beoogd rechtstreekse beïnvloeding – in de vorm van instructies – uit te sluiten, maar tevens elke vorm van indirecte beïnvloeding die de beslissingen van de toezichthoudende autoriteit zou kunnen sturen. Bovendien moeten, gelet op de door de toezichthoudende autoriteiten vervulde rol van hoeders van het recht op bescherming van de persoonlijke levenssfeer, de beslissingen van deze autoriteiten, en dus de autoriteiten zelf, boven iedere verdenking van partijdigheid verheven zijn (punten 41-43 en 52).

Het Hof heeft gepreciseerd dat een nationale toezichthoudende autoriteit, teneinde aan het criterium van onafhankelijkheid in genoemde bepaling van richtlijn 95/46 te kunnen voldoen, niet hoeft te beschikken over een autonome begrotingslijn, zoals die welke is voorzien in artikel 43, lid 3, van verordening nr. 45/2001. De lidstaten zijn immers niet verplicht om in hun nationale wettelijke regeling voorschriften op te nemen die vergelijkbaar zijn met die van hoofdstuk V van verordening nr. 45/2001 om aan hun toezichthoudende autoriteit(en) volledige onafhankelijkheid te verzekeren en zij kunnen dus bepalen dat vanuit het oogpunt van het begrotingsrecht de toezichthoudende autoriteit onder een bepaalde afdeling van een ministerie valt. De toekenning van het personeel en de materiële middelen die noodzakelijk zijn voor een dergelijke autoriteit, mag echter niet beletten dat zij haar taken „in volledige onafhankelijkheid" vervult in de zin van artikel 28, lid 1, tweede alinea, van richtlijn 95/46 (punt 58).

Arrest van 8 april 2014 (Grote kamer), Commissie/Hongarije (C-288/12, EU:C:2014:237)[79]

In deze zaak had de Commissie het Hof verzocht vast te stellen dat Hongarije, door het mandaat van de toezichthoudende autoriteit voor de bescherming van persoonsgegevens voortijdig te beëindigen, de krachtens richtlijn 95/46 op hem rustende verplichtingen niet was nagekomen.

Het Hof heeft geoordeeld dat een lidstaat die het mandaat van de toezichthoudende autoriteit voor de bescherming van persoonsgegevens voortijdig beëindigt, de krachtens richtlijn 95/46 op hem rustende verplichtingen niet nakomt (punt 62 en dictum 1).

Volgens het Hof sluit de onafhankelijkheid die de autoriteiten die belast zijn met het toezicht op de verwerking van persoonsgegevens moeten genieten, immers met name elk bevel en elke andere – rechtstreekse of indirecte – beïnvloeding van buitenaf uit, in welke vorm ook, die hun beslissingen zouden kunnen sturen en aldus de vervulling door deze autoriteiten van hun taak om een juist evenwicht tussen de bescherming van het recht op bescherming van de persoonlijke levenssfeer en het vrije verkeer van persoonsgegevens te vinden, in het gedrang zouden kunnen brengen (punt 51).

[79] Dit arrest is opgenomen in het Jaarverslag 2014, blz. 62.

Het Hof heeft voorts in herinnering gebracht dat aangezien de functionele onafhankelijkheid als zodanig niet volstaat om die toezichthoudende autoriteiten voor elke beïnvloeding van buitenaf te behoeden, het loutere gevaar dat de instanties die belast zijn met het overheidstoezicht een politieke invloed kunnen uitoefenen op de beslissingen van de toezichthoudende autoriteiten, volstaat om de onafhankelijke vervulling van de taken van deze autoriteiten te hinderen. Indien het elke lidstaat vrij zou staan om het mandaat van een toezichthoudende autoriteit vóór de aanvankelijk daarvoor voorziene afloop te beëindigen, zonder de voordien daartoe vastgestelde voorschriften en waarborgen te eerbiedigen, zou de gedurende haar gehele mandaat boven deze autoriteit hangende dreiging van een dergelijke voortijdige beëindiging kunnen leiden tot een vorm van gehoorzaamheid door haar aan de politieke macht, die onverenigbaar is met dat onafhankelijkheidsvereiste. Bovendien zou de toezichthoudende autoriteit in een dergelijke situatie niet kunnen worden geacht in alle omstandigheden boven elke verdenking van partijdigheid te functioneren (punten 52-55).

2. Vaststelling welk recht toepasselijk is en welke toezichthoudende autoriteit bevoegd is

Arrest van 1 oktober 2015, Weltimmo (C-230/14, EU:C:2015:639)[80]

De Nemzeti Adatvédelmi és Információszabadság Hatóság (nationale autoriteit belast met de gegevensbescherming en de vrijheid van informatie, Hongarije) had een geldboete opgelegd aan de in Slowakije geregistreerde vennootschap Weltimmo, die vastgoedwebsites voor in Hongarije gelegen onroerend goed beheert, omdat die vennootschap de persoonsgegevens van de adverteerders op deze websites niet had verwijderd, hoewel deze daarom hadden verzocht, en die gegevens had verstrekt aan incassobureaus opdat onbetaalde rekeningen zouden worden voldaan. Volgens de Hongaarse toezichthoudende autoriteit had Weltimmo aldus de Hongaarse wet waarbij richtlijn 95/46 was omgezet, geschonden.

Nadat aldaar cassatieberoep was ingesteld, heeft de Kúria (hoogste rechter, Hongarije) twijfels geuit over de vaststelling van het toepasselijke recht en over de bevoegdheid van de Hongaarse toezichthoudende autoriteit in het licht van artikel 4, lid 1, en artikel 28 van richtlijn 95/46. Hij heeft het Hof derhalve verscheidene prejudiciële vragen voorgelegd.

Wat het toepasselijke nationale recht betreft heeft het Hof geoordeeld dat het op grond van artikel 4, lid 1, onder a), van richtlijn 95/46 mogelijk is de wetgeving inzake de bescherming van persoonsgegevens van een andere lidstaat dan die waar de voor de verwerking van die gegevens verantwoordelijke is geregistreerd, toe te passen, voor zover bedoelde verantwoordelijke via een duurzame vestiging op het grondgebied van die lidstaat een, zelfs geringe, reële en daadwerkelijke activiteit uitoefent, in het kader waarvan die verwerking plaatsvindt. Teneinde vast te stellen of dat het geval is, kan de verwijzende rechter ten eerste met name rekening houden met het feit dat de activiteit van de voor de verwerking verantwoordelijke, in het kader waarvan deze verwerking plaatsvindt, bestaat in de exploitatie van vastgoedsites voor onroerend goed dat is gelegen op het grondgebied van die lidstaat, die in de taal van die lidstaat zijn gesteld, en dat deze activiteit dientengevolge hoofdzakelijk, zo niet volledig, op bedoelde lidstaat is gericht. De verwijzende rechter kan ten tweede tevens rekening

[80] Dit arrest is opgenomen in het Jaarverslag 2015, blz. 55.

houden met het feit dat deze verantwoordelijke in die lidstaat over een vertegenwoordiger beschikt die is belast met het innen van de uit die activiteit resulterende openstaande rekeningen en met de vertegenwoordiging van hem in bestuurlijke en juridische procedures met betrekking tot de verwerking van de betrokken gegevens. Het Hof heeft gepreciseerd dat de nationaliteit van degenen wier gegevens aldus worden verwerkt, daarentegen irrelevant is (punt 41 en dictum 1).

Wat de bevoegdheden betreft van de toezichthoudende autoriteit waarbij klachten zijn ingediend in overeenstemming met artikel 28, lid 4, van richtlijn 95/46, heeft het Hof vastgesteld dat deze autoriteit die klachten kan behandelen ongeacht het toepasselijke recht en zelfs voordat zij weet welk nationaal recht op de betrokken verwerking van toepassing is (punt 54). Evenwel kan zij, wanneer zij tot de conclusie komt dat het recht van een andere lidstaat van toepassing is, geen sancties opleggen buiten het grondgebied van de lidstaat waartoe zij behoort. In een dergelijke situatie dient zij, uit hoofde van de samenwerkingsverplichting van artikel 28, lid 6, van die richtlijn, aan de toezichthoudende autoriteit van die andere lidstaat te vragen om een mogelijke schending van dat recht vast te stellen en indien dat recht dat toestaat sancties op te leggen, waarbij zij zich in voorkomend geval kan verlaten op de informatie die zij haar zal hebben doorgegeven (punten 57, 60 en dictum 2).

3. Bevoegdheden van de nationale toezichthoudende autoriteiten

Arrest van 6 oktober 2015 (Grote kamer), Schrems (C-362/14, EU:C:2015:650)

In deze zaak (zie tevens rubriek IV, „Doorgifte van persoonsgegevens naar derde landen”) heeft het Hof met name geoordeeld dat de nationale toezichthoudende autoriteiten bevoegd zijn om de doorgifte van persoonsgegevens naar derde landen te toetsen.

In dat verband heeft het Hof om te beginnen vastgesteld dat de nationale toezichthoudende autoriteiten over een breed scala aan bevoegdheden beschikken en dat deze bevoegdheden, die niet-uitputtend zijn opgesomd in artikel 28, lid 3, van richtlijn 95/46, de middelen vormen die voor de vervulling van hun taak nodig zijn. Zo beschikken deze autoriteiten onder meer over onderzoeksbevoegdheden, zoals het recht alle inlichtingen in te winnen die voor de uitoefening van hun toezichthoudende taak noodzakelijk zijn, effectieve bevoegdheden om in te grijpen, zoals de bevoegdheid om een gegevensverwerking voorlopig of definitief te verbieden, alsmede de bevoegdheid om in rechte op te treden (punt 43).

Wat de bevoegdheid betreft om de doorgifte van persoonsgegevens naar derde landen te toetsen, heeft het Hof geoordeeld dat het juist is dat uit artikel 28, leden 1 en 6, van richtlijn 95/46 volgt dat de bevoegdheden van de nationale toezichthoudende autoriteiten betrekking hebben op de verwerking van persoonsgegevens op het grondgebied van de lidstaat waaronder zij vallen, zodat zij op grond van dit artikel 28 niet beschikken over bevoegdheden ten aanzien van de verwerking van dergelijke gegevens op het grondgebied van een derde land (punt 44).

Evenwel vormt de bewerking die bestaat in het doen doorgeven van persoonsgegevens vanuit een lidstaat naar een derde land, als zodanig echter een verwerking van persoonsgegevens die op het grondgebied van een lidstaat wordt verricht. Aangezien de nationale toezichthoudende autoriteiten ingevolge artikel 8, lid 3, van het Handvest en artikel 28 van richtlijn 95/46 belast zijn

met het toezicht op de naleving van de regels van de Unie op het gebied van de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens, is elk van hen bevoegd om na te gaan of bij een doorgifte van die gegevens naar een derde land vanuit de lidstaat waaronder zij valt, de vereisten van deze richtlijn worden nageleefd (punten 45 en 47).

Arrest van 5 juni 2018 (Grote kamer), Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388)

In dit arrest (zie tevens rubriek II.5, „Begrip ‚voor de verwerking van persoonsgegevens verantwoordelijke'"), dat onder meer betrekking heeft op de uitlegging van de artikelen 4 en 28 van richtlijn 95/46, heeft het Hof zich uitgesproken over de omvang van de bevoegdheden tot ingrijpen van de toezichthoudende autoriteiten ten aanzien van een verwerking van persoonsgegevens waarbij meerdere deelnemers betrokken zijn.

Zo heeft het Hof geoordeeld dat wanneer een buiten de Europese Unie gevestigde onderneming (zoals de Amerikaanse vennootschap Facebook) meerdere vestigingen in verschillende lidstaten heeft, de toezichthoudende autoriteit van een lidstaat bevoegd is tot uitoefening van haar bevoegdheden uit hoofde van artikel 28, lid 3, van richtlijn 95/46 ten aanzien van een vestiging van deze onderneming op het grondgebied van die lidstaat (in casu Facebook Germany), ook al is deze vestiging, ingevolge de taakverdeling binnen de groep, uitsluitend belast met de verkoop van advertentieruimte en andere marketingactiviteiten op het grondgebied van die lidstaat en berust de exclusieve verantwoordelijkheid voor de verkrijging en de verwerking van persoonsgegevens, voor het gehele grondgebied van de Europese Unie, bij een vestiging in een andere lidstaat (in casu Facebook Ireland) (punt 64 en dictum 2).

Voorts heeft het Hof gepreciseerd dat wanneer de toezichthoudende autoriteit van een lidstaat voornemens is de bevoegdheden tot ingrijpen als bedoeld in artikel 28, lid 3, van richtlijn 95/46 uit te oefenen ten aanzien van een lichaam dat gevestigd is op het grondgebied van deze lidstaat, wegens inbreuken op de regels betreffende de bescherming van persoonsgegevens die zijn begaan door een derde die voor de verwerking van deze gegevens verantwoordelijk is en waarvan de zetel zich in een andere lidstaat bevindt (in casu Facebook Ireland), deze toezichthoudende autoriteit bevoegd is de wettigheid van een dergelijke verwerking van gegevens autonoom ten opzichte van de toezichthoudende autoriteit van die laatste lidstaat (Ierland) te beoordelen, en haar bevoegdheden tot ingrijpen ten aanzien van het op haar grondgebied gevestigde lichaam kan uitoefenen zonder eerst de toezichthoudende autoriteit van de andere lidstaat te verzoeken om op te treden (punt 74 en dictum 3).

Arrest van 15 juni 2021 (Grote kamer), Facebook Ireland e.a. (C-645/19, EU:C:2021:483)

Op 11 september 2015 heeft de voorzitter van de Belgische Commissie voor de bescherming van de persoonlijke levenssfeer (hierna: „Privacycommissie") bij de Nederlandstalige rechtbank van eerste aanleg Brussel (België) een stakingsvordering ingesteld tegen Facebook Ireland, Facebook Inc. en Facebook Belgium, met als doel een einde te laten maken aan de vermeende inbreuken door Facebook op de wettelijke regeling inzake gegevensbescherming. Deze inbreuken bestonden met name in het verzamelen en gebruiken van informatie over het

surfgedrag van Belgische internetgebruikers, al dan niet houders van een Facebookaccount, door middel van verschillende technologieën, zoals cookies, social plug-ins[81] of pixels.

Op 16 februari 2018 heeft deze rechtbank zich bevoegd verklaard om uitspraak te doen over deze vordering, en ten gronde geoordeeld dat het sociale netwerk Facebook de Belgische internetgebruikers onvoldoende had geïnformeerd over de verzameling en het gebruik van de betrokken informatie. Bovendien werd de door internetgebruikers gegeven toestemming voor het verzamelen en verwerken van deze informatie als ongeldig beschouwd.

Op 2 maart 2018 hebben Facebook Ireland, Facebook Inc. en Facebook Belgium hoger beroep tegen dit vonnis ingesteld bij het hof van beroep Brussel (België), de verwijzende rechter in de onderhavige zaak. Voor deze rechterlijke instantie is de Belgische Gegevensbeschermingsautoriteit (hierna: „GBA") opgetreden als rechtsopvolger van de voorzitter van de Privacycommissie. De verwijzende rechter heeft zich uitsluitend bevoegd verklaard om uitspraak te doen op het door Facebook Belgium ingestelde hoger beroep.

De verwijzende rechter vraagt zich af wat de invloed is van de toepassing van het „één-loketmechanisme" uit de AVG[82] op de bevoegdheden van de GBA, en vraagt zich meer in het bijzonder af of de GBA voor de feiten die dateren van na de inwerkingtreding van de AVG, te weten 25 mei 2018, kan optreden tegen Facebook Belgium, aangezien Facebook Ireland als verwerkingsverantwoordelijke voor de betrokken gegevens is geïdentificeerd. Sinds die datum is namelijk, met name op grond van het in de AVG vastgelegde één-loketbeginsel, alleen de Ierse commissaris voor gegevensbescherming bevoegd om, onder toezicht van de Ierse rechterlijke instanties, een stakingsvordering in te stellen (punten 36 en 37).

In zijn arrest, gewezen door de Grote kamer, verduidelijkt het Hof de bevoegdheden van de nationale toezichthoudende autoriteiten in het kader van de AVG. Zo oordeelt het met name dat een toezichthoudende autoriteit van een lidstaat volgens deze verordening onder bepaalde voorwaarden haar bevoegdheid kan uitoefenen om elke vermeende inbreuk op de AVG voor een rechterlijke instantie van die lidstaat te brengen en in rechte op te treden met betrekking tot een grensoverschrijdende gegevensverwerking[83], ook indien zij niet de leidende autoriteit voor die verwerking is (dictum 1).

In de eerste plaats verduidelijkt het Hof de voorwaarden waaronder een nationale toezichthoudende autoriteit die niet de leidende autoriteit is met betrekking tot een grensoverschrijdende verwerking, haar bevoegdheid moet uitoefenen om elke vermeende inbreuk op de AVG voor een rechterlijke instantie van een lidstaat te brengen en, waar passend, in rechte op te treden teneinde de toepassing van die verordening te verzekeren. Zo moet de AVG die toezichthoudende autoriteit de bevoegdheid verlenen om een besluit te nemen waarbij wordt vastgesteld dat die verwerking in strijd is met de regels van die verordening, en deze bevoegdheid moet voorts worden uitgeoefend met inachtneming van de

81 Bijvoorbeeld „Vind ik leuk" of „Delen".

82 Artikel 56, lid 1, AVG luidt als volgt: „Onverminderd artikel 55 is de toezichthoudende autoriteit van de hoofdvestiging of de enige vestiging van de verwerkingsverantwoordelijke of verwerker competent op te treden als leidende toezichthoudende autoriteit voor de grensoverschrijdende verwerking door die verwerkingsverantwoordelijke of verwerker".

83 In de zin van artikel 4, punt 23, AVG.

samenwerkingsprocedure en het coherentiemechanisme die in die verordening zijn vastgelegd[84] (punt 75 en dictum 1).

Voor grensoverschrijdende verwerkingen voorziet de AVG immers in het één-loketmechanisme[85], dat is gebaseerd op een verdeling van bevoegdheden tussen een „leidende toezichthoudende autoriteit" en de andere betrokken nationale toezichthoudende autoriteiten. Dit mechanisme vereist een nauwe, loyale en doeltreffende samenwerking tussen deze autoriteiten om te zorgen voor een coherente en homogene bescherming van de regels inzake de bescherming van persoonsgegevens en aldus het nuttig effect ervan te behouden. De AVG legt in dit verband het beginsel vast van de bevoegdheid van de leidende toezichthoudende autoriteit om een besluit vast te stellen waarbij wordt geconstateerd dat een grensoverschrijdende behandeling in strijd is met de regels van die verordening[86], terwijl de bevoegdheid van de andere nationale toezichthoudende autoriteiten om een dergelijk besluit vast te stellen, zelfs voorlopig, de uitzondering vormt[87]. De leidende toezichthoudende autoriteit kan zich bij de uitoefening van haar bevoegdheden echter niet onttrekken aan een noodzakelijke dialoog en een loyale en doeltreffende samenwerking met de andere betrokken toezichthoudende autoriteiten. Daarom mag de leidende toezichthoudende autoriteit in het kader van deze samenwerking niet voorbijgaan aan de standpunten van de andere betrokken toezichthoudende autoriteiten en heeft elk relevant en gemotiveerd bezwaar van een van deze autoriteiten tot gevolg dat de vaststelling van het ontwerpbesluit van de leidende toezichthoudende autoriteit op zijn minst tijdelijk wordt geblokkeerd (punten 50-53, 56-59 en 63-65).

Het Hof verduidelijkt voorts dat de omstandigheid dat een toezichthoudende autoriteit van een lidstaat die niet de leidende toezichthoudende autoriteit is met betrekking tot een grensoverschrijdende gegevensverwerking, de bevoegdheid om elke vermeende inbreuk op de AVG voor een rechterlijke instantie van die staat te brengen en in rechte op te treden alleen kan uitoefenen met inachtneming van de regels voor de verdeling van de beslissingsbevoegdheden tussen de leidende toezichthoudende autoriteit en de andere toezichthoudende autoriteiten[88], in overeenstemming is met de artikelen 7, 8 en 47 van het Handvest, die de betrokken persoon respectievelijk bescherming van zijn persoonsgegevens en een doeltreffende voorziening in rechte waarborgen (punt 67).

In de tweede plaats oordeelt het Hof dat, wanneer sprake is van grensoverschrijdende gegevensverwerking, voor de uitoefening van de bevoegdheid van een andere toezichthoudende autoriteit dan de leidende toezichthoudende autoriteit om een rechtsvordering in te stellen[89] niet vereist is dat de in rechte gedaagde verwerkingsverantwoordelijke of verwerker die de grensoverschrijdende verwerking van persoonsgegevens verricht, op het grondgebied van die lidstaat een hoofdvestiging of een andere vestiging heeft. De uitoefening van deze bevoegdheid moet wel binnen het territoriale toepassingsgebied van de AVG[90] vallen, hetgeen veronderstelt dat de

84 Die zijn opgenomen in artikel 56 en 60 AVG.
85 Artikel 56, lid 1, AVG.
86 Artikel 60, lid 7, AVG.
87 Artikel 56, lid 2, en artikel 66 AVG voorzien in uitzonderingen op het beginsel van de beslissingsbevoegdheid van de leidende toezichthoudende autoriteit.
88 Die zijn vastgelegd in de artikelen 55 en 56, gelezen in samenhang met artikel 60 AVG.
89 Op grond van artikel 58, lid 5, AVG.
90 Artikel 3, lid 1, AVG bepaalt dat deze verordening van toepassing is op de verwerking van persoonsgegevens „in het kader van activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie, ongeacht of de verwerking in de Unie plaatsvindt".

verwerkingsverantwoordelijke of de verwerker die de grensoverschrijdende verwerking verricht over een vestiging op het grondgebied van de Unie beschikt (punten 80, 83, 84 en dictum 2).

In de derde plaats verklaart het Hof voor recht dat de bevoegdheid van een andere toezichthoudende autoriteit van een lidstaat dan de leidende toezichthoudende autoriteit om elke vermeende inbreuk op de AVG voor een rechterlijke instantie van die lidstaat te brengen en, waar passend, een rechtsvordering in te stellen, in geval van grensoverschrijdende gegevensverwerking zowel kan worden uitgeoefend ten aanzien van de hoofdvestiging van de verwerkingsverantwoordelijke die zich in de lidstaat van die autoriteit bevindt, als ten aanzien van een andere vestiging van die verantwoordelijke, voor zover de rechtsvordering ziet op gegevensverwerking die plaatsvindt in het kader van de activiteiten van die vestiging en die autoriteit competent is om die bevoegdheid uit te oefenen.

Het Hof preciseert echter dat voor de uitoefening van deze bevoegdheid vereist is dat de AVG van toepassing is. In casu houden de activiteiten van de Belgische vestiging van de Facebook-groep onlosmakelijk verband met de verwerking van de persoonsgegevens die in het hoofdgeding aan de orde is, waarvoor Facebook Ireland voor het grondgebied van de Unie verantwoordelijk is, zodat deze verwerking wordt verricht „in het kader van de activiteiten van een vestiging van de verwerkingsverantwoordelijke" en dus wel degelijk binnen de werkingssfeer van de AVG valt (punten 94-96 en dictum 3).

In de vierde plaats oordeelt het Hof dat wanneer een toezichthoudende autoriteit van een lidstaat die niet de „leidende toezichthoudende autoriteit" is, vóór de inwerkingtreding van de AVG een rechtsvordering heeft ingesteld met betrekking tot een grensoverschrijdende verwerking van persoonsgegevens, die vordering krachtens het Unierecht kan worden gehandhaafd op grond van de bepalingen van richtlijn 95/46, die van toepassing blijft met betrekking tot inbreuken op de daarin vastgestelde regels die zijn begaan tot de datum van intrekking van die richtlijn. Bovendien kan deze autoriteit deze vordering instellen voor inbreuken die zijn begaan na de datum van inwerkingtreding van de AVG, voor zover dit gebeurt in een van de situaties waarin die verordening diezelfde autoriteit bij wijze van uitzondering de bevoegdheid verleent om een besluit te nemen waarbij wordt vastgesteld dat de betrokken gegevensverwerking in strijd is met de regels van die verordening, en mits zij daarbij de in die verordening vastgelegde samenwerkingsprocedure en het coherentiemechanisme in acht neemt (punt 105 en dictum 4).

In de vijfde en laatste plaats erkent het Hof de rechtstreekse werking van de bepaling van de AVG op grond waarvan elke lidstaat bij wet bepaalt dat zijn toezichthoudende autoriteit bevoegd is om elke inbreuk op deze verordening ter kennis te brengen van de gerechtelijke autoriteiten en, waar passend, in rechte op te treden. Bijgevolg kan een dergelijke autoriteit zich op deze bepaling beroepen om een vordering tegen particulieren in te leiden of voort te zetten, ook al is zij niet specifiek omgezet in de wetgeving van de betrokken lidstaat (punt 113 en dictum 5).

VII. Territoriale toepassing van de Europese wettelijke regeling

Arrest van 13 mei 2014 (Grote kamer), Google Spain en Google (C-131/12, EU:C:2014:317)

In dit arrest [zie tevens de rubrieken II.3, „Begrip ‚verwerking van persoonsgegevens'", en V.1, „Recht van verzet tegen de verwerking van persoonsgegevens (‚recht om te worden vergeten')"] heeft het Hof zich tevens uitgesproken over de territoriale werkingssfeer van richtlijn 95/46.

Zo heeft het Hof geoordeeld dat er sprake is van een verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van de voor de verwerking verantwoordelijke op het grondgebied van de lidstaat, in de zin van richtlijn 95/46, wanneer de exploitant van een zoekmachine die zijn maatschappelijke zetel weliswaar in een derde land heeft, in een lidstaat ten behoeve van het promoten en de verkoop van door deze zoekmachine aangeboden advertentieruimte een bijkantoor of een dochteronderneming opricht waarvan de activiteiten op de inwoners van die lidstaat zijn gericht (punten 55, 60 en dictum 2).

In dergelijke omstandigheden zijn de activiteiten van de exploitant van de zoekmachine en die van zijn vestiging in de betrokken lidstaat, hoewel zij verschillend zijn, immers onlosmakelijk met elkaar verbonden, daar de activiteiten inzake de advertentieruimtes het middel vormen om de betrokken zoekmachine economisch rendabel te maken en deze machine tegelijkertijd het middel is waarmee deze activiteiten kunnen worden verricht (punt 56).

VIII. Recht van het publiek op toegang tot documenten van instellingen van de Europese Unie en bescherming van persoonsgegevens

Arrest van 29 juni 2010 (Grote kamer), Commissie/Bavarian Lager (C-28/08 P, EU:C:2010:378)

Bavarian Lager, een vennootschap die was opgericht met als doel Duits bier te importeren voor verkoop in cafés en bars in het Verenigd Koninkrijk, kon haar product niet verkopen, doordat een groot aantal cafés en bars in het Verenigd Koninkrijk gebonden waren door exclusieve afnameovereenkomsten op grond waarvan zij hun bier moesten betrekken van bepaalde brouwerijen.

Krachtens de regeling van het Verenigd Koninkrijk inzake levering van bier (hierna: „GBP"), waren Britse brouwerijen gehouden de houders van pubs de mogelijkheid te bieden, bier van een andere brouwerij te betrekken, mits het was gefust. Het meeste buiten het Verenigd Koninkrijk geproduceerde bier kon niet als „bier op fust" in de zin van de GBP worden beschouwd, zodat het niet binnen de werkingssfeer ervan viel. Daar zij van mening was dat deze regeling een maatregel van gelijke werking als een kwantitatieve invoerbeperking vormde, had Bavarian Lager een klacht ingediend bij de Commissie.

Tijdens de door de Commissie tegen het Verenigd Koninkrijk ingeleide niet-nakomingsprocedure, hebben vertegenwoordigers van de communautaire en de Britse overheid alsmede vertegenwoordigers van de Confédération des Brasseurs du Marché Commun (confederatie van brouwers van de gemeenschappelijke markt, CBMC) deelgenomen aan een vergadering die plaatsvond op 11 oktober 1996. Na door de Britse autoriteiten op de hoogte te zijn gebracht van de wijziging in de betrokken regeling, die ertoe strekte de verkoop van flessenbier als bier van een andere oorsprong, net als bier op fust, mogelijk te maken, had de Commissie Bavarian Lager in kennis gesteld van de schorsing van de niet-nakomingsprocedure.

Nadat Bavarian Lager een verzoek had ingediend teneinde het volledige proces-verbaal van de vergadering van oktober 1996, met vermelding de namen van alle deelnemers, te verkrijgen, heeft de Commissie dit verzoek afgewezen bij besluit van 18 maart 2004, waarbij zij zich met name beriep op de bescherming van de persoonlijke levenssfeer van deze personen, zoals gewaarborgd bij verordening 45/2001.

Bavarian Lager heeft vervolgens beroep ingesteld bij het Gerecht en om nietigverklaring van dat besluit van de Commissie verzocht. Bij arrest van 8 november 2007 heeft het Gerecht het besluit van de Commissie nietig verklaard, met name op grond van de overweging dat de enkele opname van de naam van de betrokkenen op de lijst van personen die namens de entiteit die zij vertegenwoordigen hebben deelgenomen aan een vergadering, geen inbreuk vormde en de persoonlijke levenssfeer van deze personen niet in gevaar bracht. De Commissie, ondersteund door het Verenigd Koninkrijk en de Raad, heeft daarop bij het Hof een hogere voorziening ingesteld tegen dat arrest van het Gerecht.

Het Hof heeft om te beginnen opgemerkt dat wanneer een verzoek dat is gebaseerd op verordening nr. 1049/2001[91] inzake de toegang tot documenten, strekt tot het verkrijgen van toegang tot documenten die persoonsgegevens bevatten, de bepalingen van verordening nr. 45/2001 in volle omvang van toepassing worden, met inbegrip van de bepaling volgens welke de ontvanger van de door te geven persoonsgegevens de noodzaak van openbaarmaking moet aantonen, en de bepaling die de betrokkene de mogelijkheid biedt om op grond van zwaarwegende en gerechtvaardigde redenen die met zijn bijzondere situatie verband houden, te allen tijde bezwaar aan te tekenen tegen de verwerking van hem betreffende gegevens (punt 63).

Vervolgens heeft het Hof vastgesteld dat de lijst van deelnemers aan een in het kader van een niet-nakomingsprocedure gehouden vergadering, welke lijst is opgenomen in het proces-verbaal van die vergadering, persoonsgegevens bevatte in de zin van artikel 2, onder a), van verordening nr. 45/2001, daar de personen die aan de vergadering hebben kunnen deelnemen, konden worden geïdentificeerd (punt 70).

Ten slotte kwam het Hof tot de slotsom dat, door te eisen dat voor de personen die niet uitdrukkelijk toestemming hadden gegeven voor de openbaarmaking van de op hen betrekking hebbende persoonsgegevens in het proces-verbaal, de noodzaak van de doorgifte van deze

[91] Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van 30 mei 2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie (PB 2001, L 145, blz. 43).

persoonsgegevens werd aangetoond, de Commissie had gehandeld in overeenstemming met artikel 8, onder b), van verordening nr. 45/2001 (punt 77).

Wanneer in het kader van een verzoek om toegang tot dat proces-verbaal uit hoofde van verordening nr. 1049/2001 geen enkele uitdrukkelijke en legitieme rechtvaardigingsgrond en evenmin enig overtuigend argument tot staving van de noodzaak van de doorgifte van deze persoonsgegevens is aangevoerd, kan de Commissie immers de verschillende belangen van de betrokken partijen niet tegen elkaar afwegen. Evenmin kan zij nagaan of er redenen bestaan om aan te nemen dat door deze doorgifte de rechtmatige belangen van de betrokkenen worden geschaad, zoals artikel 8, onder b), van verordening nr. 45/2001 voorschrijft (punt 78).[92]

Arrest van 16 juli 2015, ClientEarth en PAN Europe/EFSA (C-615/13 P, EU:C:2015:489)

De Europese Autoriteit voor voedselveiligheid (EFSA) had een werkgroep opgericht teneinde richtsnoeren op te stellen waarin de toepassing van artikel 8, lid 5, van verordening (EG) nr. 1107/2009[93] werd uitgewerkt. Volgens dat artikel doet de aanvrager van toelating voor het op de markt brengen van een gewasbeschermingsmiddel het dossier vergezeld gaan van alle collegiaal getoetste wetenschappelijke open literatuur, zoals vastgesteld door EFSA, over de neveneffecten van de werkzame stof en de relevante metabolieten daarvan voor de gezondheid, het milieu en niet-doelsoorten.

Daar over de ontwerprichtsnoeren een openbare raadpleging was gehouden, hadden ClientEarth en Pesticide Action Network Europe (PAN Europe) opmerkingen over dat ontwerp ingediend. In deze context hadden zij EFSA gezamenlijk verzocht om toegang tot verschillende documenten over de voorbereiding van de ontwerprichtsnoeren, met inbegrip van de opmerkingen van de externe deskundigen.

EFSA had ClientEarth en PAN Europe toegang verleend tot met name de individuele opmerkingen van de externe deskundigen over de ontwerprichtsnoeren. Zij wees er echter op dat zij de namen van deze deskundigen onleesbaar had gemaakt overeenkomstig artikel 4, lid 1, onder b), van verordening nr. 1049/2001 en de Uniewetgeving inzake bescherming van persoonsgegevens, met name verordening nr. 45/2001. Zij wees er in dat verband op dat openbaarmaking van de namen van die deskundigen een doorgifte van persoonsgegevens inhield in de zin van artikel 8 van verordening nr. 45/2001, en dat in casu niet was voldaan aan de in dat artikel genoemde voorwaarden voor een dergelijke doorgifte.

Daarop hebben ClientEarth en PAN Europe bij het Gerecht beroep in gesteld strekkende tot nietigverklaring van dat besluit van EFSA. Daar het Gerecht dit beroep had verworpen, hebben ClientEarth en PAN Europe bij het Hof een hogere voorziening ingesteld tegen het arrest[94] van het Gerecht.

In de eerste plaats heeft het Hof opgemerkt dat aangezien de gevraagde informatie het mogelijk zou maken een bepaalde deskundige met bepaalde opmerkingen in verband te brengen, zij

92 Dit arrest is opgenomen in het Jaarverslag 2010, blz. 14.

93 Verordening (EG) nr. 1107/2009 van het Europees Parlement en de Raad van 21 oktober 2009 betreffende het op de markt brengen van gewasbeschermingsmiddelen en tot intrekking van de richtlijnen 79/117/EEG en 91/414/EEG van de Raad (PB 2009, L 309, blz. 1).

94 Arrest Gerecht van 13 september 2013, ClientEarth en PAN Europe/EFSA (T-214/11, EU:T:2013:483).

betrekking heeft op geïdentificeerde natuurlijke personen en zij dus een geheel van persoonsgegevens vormt in de zin van artikel 2, onder a), van verordening nr. 45/2001. Daar de begrippen „persoonsgegevens" in de zin van artikel 2, onder a), van verordening nr. 45/2001 en „gegevens betreffende de persoonlijke levenssfeer" niet mogen worden verward, heeft het Hof voorts vastgesteld dat de bewering van ClientEarth en PAN Europe dat de litigieuze informatie geen betrekking had op de persoonlijke levenssfeer van de betrokken deskundigen, niet ter zake dienend was (punten 29 en 32).

In de tweede plaats heeft het Hof het argument van ClientEarth en PAN Europe onderzocht dat was gebaseerd op het bestaan van een klimaat van wantrouwen ten aanzien van EFSA, die vaak wordt beschuldigd van partijdigheid op grond dat zij een beroep doet op deskundigen die persoonlijke belangen hebben die zijn ingegeven door hun banden met de industrie, en op de noodzaak om de transparantie van het besluitvormingsproces van die autoriteit te waarborgen. Dit argument was gestaafd door een studie waarin was vastgesteld dat er banden bestonden tussen de meerderheid van de leden van een uit deskundigen samengestelde werkgroep van EFSA en industriële belangengroepen. In dit verband heeft het Hof geoordeeld dat het verkrijgen van de litigieuze informatie noodzakelijk was om de onpartijdigheid van elke deskundige in de uitvoering van zijn wetenschappelijke taak ten dienste van EFSA concreet na te kunnen gaan. Bijgevolg heeft het Hof het arrest van het Gerecht vernietigd en daarbij vastgesteld dat het Gerecht ten onrechte had geoordeeld dat bovenbedoeld argument van ClientEarth en PAN Europe niet volstond om aan te tonen dat de doorgifte van de litigieuze informatie noodzakelijk was (punten 57-59).

In de derde plaats, teneinde te beoordelen of het litigieuze besluit van EFSA rechtmatig was, heeft het Hof onderzocht of er een reden bestond om aan te nemen dat die doorgifte de rechtmatige belangen van de betrokkenen had kunnen schaden. In dit verband heeft het Hof vastgesteld dat de bewering van EFSA dat openbaarmaking van de litigieuze informatie de persoonlijke levenssfeer en integriteit van die deskundigen had kunnen schaden, een algemene overweging betrof die voor het overige door geen enkel concreet gegeven werd gestaafd. Het Hof was van oordeel dat een dergelijke openbaarmaking integendeel op zich de betrokken vermoedens van partijdigheid had kunnen wegnemen of de eventueel betrokken deskundigen de mogelijkheid had geboden om, in voorkomend geval door middel van de beschikbare beroepswegen, de gegrondheid van die beschuldigingen van partijdigheid te betwisten. Gelet op deze gegevens heeft het Hof ook het besluit van EFSA nietig verklaard (punten 69 en 73).

* * *

De arresten in deze fiche zijn geïndexeerd in het Repertorium van de rechtspraak in de rubrieken 1.04.03.07, 1.04.03.08, 1.04.03.10, 1.04.03.11, 2.04, 2.05.00, 4.11.01, 4.11.07, 4.11.11.01.