HOF VAN JUSTITIE
VAN DE EUROPESE UNIE

NL

Themafiche
Bescherming van persoonsgegevens

Directie Onderzoek en Documentatie

curia.europa.eu

Voorwoord

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 primaire recht, met name in artikel 8 van het Handvest van de grondrechten van de Europese Unie (hierna: „Handvest") en in artikel 16, lid 1, van het Verdrag betreffende de werking van de Europese Unie (VWEU). 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.

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 in 2018 is ingetrokken, vormde in dit opzicht de belangrijkste Uniehandeling op dat gebied.

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 zij dat, teneinde rekening te houden met nieuwe technologische en marktontwikkelingen, de Uniewetgever in 2017 een aanvang heeft gemaakt met de evaluatie van deze richtlijn[4], die tot op heden nog steeds aan de gang is[5].

In 2016 heeft de Europese Unie het algemene rechtskader op dit gebied herzien. Daartoe heeft de Unie verordening (EU) 2016/679 [6] betreffende de bescherming van

---

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 6).

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, „Overeenstemming van het afgeleide Unierecht met het recht op bescherming van persoonsgegevens", van deze fiche).

4 De Commissie heeft op 10 januari 2017 een voorstel ingediend ter vervanging van die richtlijn door een verordening betreffende privacy en elektronische communicatie.

5 Op 10 februari 2021 heeft de Raad van de Europese Unie zijn goedkeuring gehecht aan een onderhandelingsmandaat voor de herziening van de regels inzake privacy en vertrouwelijkheid bij het gebruik van elektronischecommunicatiediensten, zodat onderhandelingen met het Europees Parlement kunnen worden gestart. De tekst van het 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 (e-privacyverordening), is beschikbaar via deze link: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN*.

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).

persoonsgegevens (hierna: „AVG") vastgesteld, waarbij richtlijn 95/46 is ingetrokken en die sinds 25 mei 2018 van toepassing is, en richtlijn (EU) 2016/680 [7] inzake bescherming van die gegevens in strafzaken, waarvan de bepalingen van toepassing zijn sinds 6 mei 2018.

Wat de verwerking van persoonsgegevens door de instellingen en organen van de Unie betreft wordt de bescherming van deze gegevens, sinds 11 december 2018, gewaarborgd door verordening (EU) 2018/1725.[8] In het belang van een coherente benadering van de bescherming van persoonsgegevens in de gehele Unie, beoogt deze verordening de desbetreffende voorschriften zoveel mogelijk aan te passen aan het bij de AVG ingevoerde stelsel.

Ten slotte heeft de Uniewetgever, om het hoofd te bieden aan de uitdagingen die de nieuwe technologieën met zich meebrengen, sinds 2020 gewerkt aan de vaststelling van nieuwe wettelijke maatregelen[9] die aansluiten bij de Unierechtelijke bepalingen inzake de bescherming van persoonsgegevens.

In het licht van de uitgebreide rechtspraak van het Hof van Justitie op het gebied van de bescherming van persoonsgegevens, beoogt deze themafiche een selectie te geven van de fundamentele arresten op dit gebied en van arresten die een belangrijke bijdrage hebben geleverd aan de ontwikkeling van deze rechtspraak, waarbij bijzondere aandacht wordt geschonken aan de arresten van de Grote kamer van het Hof. Meer in het bijzonder bestrijkt deze fiche zowel de rechtspraak inzake de algemene regelgeving op het gebied van de bescherming van persoonsgegevens, die is voortgekomen uit de uitlegging van richtlijn 95/46 en van de AVG, als de rechtspraak inzake de sectorspecifieke regelgeving, die met name betrekking heeft op de sector elektronische communicatie en het strafrecht. Voorts beoogt deze fiche een selectie te maken van arresten die betrekking hebben op regelingen die horizontaal van toepassing zijn, waarbij van meet af aan de doorslaggevende rol van het Handvest in de ontwikkeling van de rechtspraak voor het voetlicht wordt gebracht.

---

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 (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 (PB 2018, L 295, blz. 39).

9 In dit verband moet met name worden gewezen op drie wetgevingsinitiatieven: *i)* verordening (EU) 2022/868 van het Europees Parlement en de Raad van 30 mei 2022 betreffende Europese datagovernance en tot wijziging van verordening (EU) 2018/1724 (datagovernanceverordening) (PB 2022, L 152, blz. 1) en verordening (EU) 2023/2854 van het Europees Parlement en de Raad van 13 december 2023 betreffende geharmoniseerde regels inzake eerlijke toegang tot en eerlijk gebruik van gegevens en tot wijziging van verordening (EU) 2017/2394 en richtlijn (EU) 2020/1828 (dataverordening) (PB 2023, L 2854, blz. 1), *ii)* een wetgevingspakket betreffende digitale diensten en markten, bestaande uit verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van richtlijn 2000/31/EG (digitaledienstenverordening) (PB 2022, L 277, blz. 1) en uit verordening (EU) 2022/1925 van het Europees Parlement en de Raad van 14 september 2022 over betwistbare en eerlijke markten in de digitale sector, en tot wijziging van richtlijnen (EU) 2019/1937 en (EU) 2020/1828 (digitalemarktenverordening) (PB 2022, L 265, blz. 1), en *iii)* het allereerste wetgevingsvoorstel voor een regelgevend kader op het gebied van artificiële intelligentie, dat concrete vorm heeft aangenomen in een verordening betreffende artificiële intelligentie (PB 2024, L, 1689).

Inhoudsopgave

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).

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). Deze landbouwers verzetten zich tegen deze bekendmaking met het argument, in het bijzonder, dat zij 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 [10] en nr. 259/2008 [11], 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 (EG) nr. 1290/2005 en van verordening (EG) 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 betrokken begunstigden op eerbiediging van hun privéleven in het algemeen en op de bescherming van hun persoonsgegevens in het bijzonder.

---

[10] 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).

[11] 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).

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. 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.

Het Hof heeft dus bepaalde voorschriften van verordening (EG) nr. 1290/2005 alsmede verordening (EG) 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. 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.

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***)***

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 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 elektronischecommunicatiediensten 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 hoeveel malen de abonnee of de geregistreerde gebruiker gedurende een specifieke periode met bepaalde personen heeft gecommuniceerd.

Het Hof heeft om te beginnen geoordeeld dat de bepalingen van richtlijn 2006/24, doordat zij deze aanbieders dergelijke verplichtingen opleggen, een bijzonder zware inmenging vormden in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten op eerbiediging van het privéleven en op bescherming van persoonsgegevens. 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.

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. Richtlijn 2006/24 bestreek immers algemeen elke persoon en alle elektronischecommunicatiemiddelen 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. 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. 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.

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.

Arrest van 21 juni 2022 (Grote kamer), Ligue des droits humains (C-817/19, EU:C:2022:491)

PNR-gegevens (of voluit „Passenger Name Record”-gegevens) zijn reserveringsgegevens die luchtvaartmaatschappijen opslaan in hun reserverings- en vertrekcontrolesystemen. De PNR-richtlijn[12] legt die maatschappijen de verplichting op om de gegevens van elke passagier die een vlucht naar of vanuit een derde land neemt door te geven aan de passagiersinformatie-eenheid (hierna: „PIE”) van de betrokken lidstaat van aankomst of vertrek, teneinde terrorisme en ernstige criminaliteit te bestrijden. De doorgegeven PNR-gegevens worden namelijk op voorhand beoordeeld door de PIE[13] en worden vervolgens bewaard, zodat zij eventueel achteraf nog kunnen worden beoordeeld door de bevoegde autoriteiten van de betrokken lidstaat of van een andere lidstaat. De lidstaten kunnen beslissen om de richtlijn ook op vluchten binnen de Unie toe te passen[14].

De Ligue des droits humains heeft bij het Grondwettelijk Hof (België) beroep ingesteld tot vernietiging van de Belgische wet waarbij zowel de PNR-richtlijn als de API-richtlijn[15] in nationaal recht zijn omgezet. Volgens verzoekster schendt deze wet het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens. Zij bekritiseert het feit dat die wet de PNR-gegevens zeer ruim omschrijft en het mogelijk

---

12 Richtlijn (EU) 2016/681 van het Europees Parlement en de Raad van 27 april 2016 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit (PB 2016, L 119, blz. 132) (hierna: „PNR-richtlijn”).

13 Deze beoordeling op voorhand beoogt te bepalen welke personen moeten worden onderworpen aan een nader onderzoek door de bevoegde instanties omdat zij betrokken zouden kunnen zijn bij een terroristisch misdrijf of bij ernstige criminaliteit. Zij wordt systematisch en geautomatiseerd uitgevoerd door de PNR-gegevens te vergelijken met „nuttige” databanken dan wel ze te verwerken aan de hand van vooraf in artikel 6, lid 2, onder a), en lid 3, van de PNR-richtlijn vastgestelde criteria.

14 Door gebruik te maken van de door artikel 2 van de PNR-richtlijn geboden mogelijkheid.

15 Richtlijn 2004/82/EG van de Raad van 29 april 2004 betreffende de verplichting voor vervoerders om passagiersgegevens door te geven (PB 2004, L 261, blz. 24) (hierna: „API-richtlijn”). Deze richtlijn regelt de verstrekking vooraf van passagiersgegevens (advance passenger information data – zoals het soort gebruikte reisdocument en het nummer ervan alsmede de nationaliteit) door luchtvaartmaatschappijen aan de bevoegde nationale instanties, ter verbetering van de grenscontroles en ter bestrijding van illegale immigratie.

maakt om de gegevens van álle passagiers te verzamelen, door te geven en te verwerken. De wet is volgens haar ook in strijd met het vrije verkeer van personen, aangezien het PNR-systeem daarin wordt uitgebreid naar vluchten en andere soorten vervoer binnen de Unie en op die manier indirect opnieuw grenscontroles worden ingevoerd.

In deze context heeft het Belgische Grondwettelijk Hof het Hof om een prejudiciële beslissing verzocht over onder meer vragen met betrekking tot de geldigheid van de PNR-richtlijn.

In zijn arrest bevestigt het Hof (Grote kamer) de geldigheid van de PNR-richtlijn voor zover deze kan worden uitgelegd in overeenstemming met het Handvest.

Dienaangaande oordeelt het Hof dat het onderzoek van de gestelde vragen niets aan het licht heeft gebracht dat de geldigheid van de PNR-richtlijn kan aantasten, aangezien de uitlegging die het van deze richtlijn heeft gegeven in het licht van de grondrechten die worden gewaarborgd door de artikelen 7, 8 en 21 en artikel 52, lid 1, van het Handvest[16], garandeert dat die richtlijn in overeenstemming is met deze artikelen.

Om te beginnen herinnert het Hof eraan dat een Unieregeling zoveel mogelijk zodanig moet worden uitgelegd dat geen afbreuk wordt gedaan aan de geldigheid van deze regeling en dat zij in overeenstemming is met het gehele primaire recht, en met name het Handvest. De lidstaten moeten er dan ook op toezien dat zij zich niet baseren op een uitlegging van het Handvest die in conflict komt met de grondrechten die door de rechtsorde van de Unie worden beschermd of met de andere algemene beginselen die in deze rechtsorde worden erkend. Het Hof verduidelijkt dat een groot aantal overwegingen en bepalingen van de PNR-richtlijn een dergelijke conforme uitlegging vereist en benadrukt dat de verwijzing daarin naar een hoog niveau van gegevensbescherming laat zien dat de Uniewetgever het erg belangrijk vindt dat de in het Handvest verankerde grondrechten ten volle worden geëerbiedigd.

Het Hof constateert dat de PNR-richtlijn inmengingen van een zekere ernst met zich meebrengt in de grondrechten die worden gewaarborgd door de artikelen 7 en 8 van het Handvest, vooral omdat zij een systeem van permanente, niet-gerichte en systematische controle beoogt in te voeren waarbij de persoonsgegevens van iedereen die luchtvervoerdiensten gebruikt automatisch worden beoordeeld. Het wijst erop dat voor de vraag of de lidstaten een dergelijke inmenging kunnen rechtvaardigen, moet worden nagegaan wat de ernst van de inmenging is en of de nagestreefde doelstelling van algemeen belang in verhouding staat tot die ernst.

Het Hof komt tot de conclusie dat de doorgifte, de verwerking en de bewaring van PNR-gegevens waarin die richtlijn voorziet kunnen worden geacht niet verder te gaan dan strikt noodzakelijk is om terroristische misdrijven en ernstige criminaliteit te bestrijden,

---

[16] Volgens deze bepaling moeten beperkingen op de uitoefening van de in dit Handvest erkende rechten en vrijheden bij wet worden gesteld en de wezenlijke inhoud ervan eerbiedigen. Bovendien kunnen slechts beperkingen op die rechten en vrijheden worden gesteld, indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.

op voorwaarde dat de bevoegdheden die de richtlijn verleent, eng worden uitgelegd. Het arrest van 21 juni 2022 verduidelijkt in dit verband met name het volgende:

- Het bij de PNR-richtlijn ingevoerde systeem mag enkel gelden voor de gegevens die in de rubrieken van bijlage I bij deze richtlijn duidelijk worden aangegeven en afgebakend en die verband houden met de betrokken vlucht en passagier, wat voor bepaalde rubrieken betekent dat het enkel gaat om de gegevens die daar uitdrukkelijk in worden vermeld.[17]
- Het systeem van deze richtlijn mag alleen worden toegepast op terroristische misdrijven en ernstige vormen van criminaliteit die minstens indirect een objectief verband vertonen met het luchtvervoer van passagiers. Dit systeem mag niet worden uitgebreid naar strafbare feiten die weliswaar voldoen aan het in de richtlijn gehanteerde ernstcriterium en meer bepaald worden genoemd in bijlage II daarbij, maar wegens de specifieke kenmerken van het nationale strafrechtsysteem gewone criminaliteit vormen.
- Wanneer een lidstaat gebruikmaakt van de mogelijkheid die de PNR-richtlijn biedt om deze richtlijn bij uitbreiding toe te passen op alle of een deel van de vluchten binnen de Unie, mag dit niet verder gaan dan strikt noodzakelijk is. Op deze beslissing moet effectief controle kunnen worden uitgeoefend door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is. Het Hof zet in dit verband uiteen dat:
  - slechts wanneer een lidstaat vaststelt dat er voldoende concrete omstandigheden zijn om aan te nemen dat hij te maken heeft met een werkelijke en actuele of voorzienbare terroristische dreiging, de grenzen van het strikt noodzakelijke niet worden overschreden wanneer deze richtlijn gedurende een periode die tot het strikt noodzakelijke beperkt is maar kan worden verlengd, wordt toegepast op alle vluchten binnen de Unie die worden uitgevoerd van of naar deze lidstaat.[18]

  - een lidstaat die niet met een dergelijke terroristische dreiging wordt geconfronteerd, kan de toepassing van die richtlijn niet uitbreiden naar alle vluchten binnen de Unie, maar enkel naar vluchten binnen de Unie die betrekking hebben op bepaalde verbindingen, reisroutes of luchthavens waarvoor er volgens die lidstaat aanwijzingen bestaan dat de uitbreiding gerechtvaardigd is. Of de uitbreiding naar de geselecteerde vluchten in kwestie strikt noodzakelijk is, moet regelmatig opnieuw worden bekeken in het licht van wijzigingen in de omstandigheden die hun selectie aanvankelijk rechtvaardigden.

---

[17] Zo mag met name de „betalingsinformatie" (rubriek 6 van de bijlage) enkel betrekking hebben op de betalingswijzen en de facturatie van het vliegticket, en geen andere informatie omvatten die geen rechtstreeks verband houdt met de vlucht, en mogen de „algemene opmerkingen" (rubriek 12) enkel slaan op de gegevens betreffende de minderjarige vliegtuigpassagier die in deze rubriek uitdrukkelijk worden genoemd.

[18] Het bestaan van een dergelijke bedreiging toont immers op zichzelf een verband aan tussen de doorgifte en de verwerking van de betrokken gegevens enerzijds en de bestrijding van terrorisme anderzijds. Het feit dat een lidstaat de PNR-richtlijn voor een beperkte duur wil toepassen op alle vluchten binnen de EU van of naar de betrokken lidstaat, gaat dus niet verder dan strikt noodzakelijk is, aangezien de beslissing die in deze toepassing voorziet, door een rechterlijke instantie of een onafhankelijke administratieve entiteit moet kunnen worden getoetst.

- Bij de voorafgaande beoordeling van de PNR-gegevens, die tot doel heeft te bepalen welke personen vóór hun aankomst of vertrek nader moeten worden onderzocht, en die in eerste instantie via geautomatiseerde verwerkingen wordt uitgevoerd, mag de PIE deze gegevens enkel vergelijken met databanken voor gezochte of gesignaleerde personen of voorwerpen.[19] Deze databanken mogen niet discrimineren en moeten door de bevoegde autoriteiten worden gebruikt om terroristische misdrijven en ernstige vormen van criminaliteit te bestrijden die minstens indirect een objectief verband vertonen met het luchtvervoer van passagiers. Wanneer de PIE een voorafgaande beoordeling uitvoert aan de hand van vooraf bepaalde criteria, mag zij geen kunstmatige-intelligentietechnologieën zoals machinaal leren (machine learning) gebruiken, aangezien deze zonder menselijke tussenkomst of controle aanpassingen kunnen doorvoeren in het beoordelingsproces en met name in de beoordelingscriteria waarop de resultaten van dat proces zijn gebaseerd, alsook in de weging van deze criteria. Vooraf bepaalde criteria moeten zodanig worden gekozen dat zij specifiek gericht zijn op individuen van wie redelijkerwijs kan worden vermoed dat zij betrokken zijn bij terroristische misdrijven of ernstige criminaliteit, dat zowel „belastende" als „ontlastende" elementen in aanmerking worden genomen en dat geen directe of indirecte discriminatie wordt gecreëerd.[20]
- Gezien de foutenmarge die inherent is aan dergelijke geautomatiseerde verwerkingen van PNR-gegevens en het vrij grote aantal „vals-positieve" resultaten dat deze in 2018 en 2019 hebben opgeleverd, hangt de geschiktheid van het door de PNR-richtlijn ingevoerde systeem om de beoogde doelstellingen te bereiken voornamelijk af van het goede verloop van de controle op de middels die verwerkingen verkregen positieve resultaten, die de PIE in tweede instantie op niet-geautomatiseerde wijze verricht. De lidstaten moeten voor het personeel van de PIE dat met deze afzonderlijke tweede controle is belast, duidelijke en nauwkeurige richtsnoeren vaststellen om ervoor te zorgen dat de grondrechten die worden gewaarborgd door de artikelen 7, 8 en 21 van het Handvest ten volle worden geëerbiedigd en, in het bijzonder, dat binnen de PIE een coherente administratieve praktijk wordt gevolgd waarbij het non-discriminatiebeginsel in acht wordt genomen. De lidstaten moeten er met name op toezien dat de PIE objectieve controlecriteria vastlegt waarmee haar personeel kan nagaan of en in hoeverre een positieve overeenkomst (hit) daadwerkelijk iemand betreft die mogelijkerwijs betrokken is bij terroristische misdrijven of ernstige criminaliteit, en of de automatische verwerkingen niet-discriminerend zijn. Het Hof benadrukt in deze context ook dat de bevoegde autoriteiten zich ervan moeten vergewissen

---

[19] Te weten databanken betreffende gezochte of gesignaleerde personen of voorwerpen in de zin van artikel 6, lid 3, onder a), van de PNR-richtlijn. Beoordelingen aan de hand van verschillende databanken kunnen daarentegen de vorm aannemen van informatievergaring (*data mining*) en in een overmatig gebruik van de PNR-gegevens kunnen resulteren daar zij de mogelijkheid bieden om een precies profiel op te stellen van eenieder die gewoon de intentie heeft een vliegtuig te nemen.

[20] De vooraf bepaalde criteria moeten doelgericht, evenredig en specifiek zijn en moeten regelmatig worden getoetst (artikel 6, lid 4, van de PNR-richtlijn). De voorafgaande beoordeling aan de hand van vooraf bepaalde criteria moet op niet-discriminerende wijze worden verricht. Volgens artikel 6, lid 4, vierde volzin, van de PNR-richtlijn mogen de criteria onder geen beding gebaseerd zijn op ras, etnische afstamming, religieuze, levensbeschouwelijke of politieke overtuiging, vakbondslidmaatschap, gezondheid, seksleven of seksuele geaardheid van de betrokkene.

dat de betrokkene kan begrijpen hoe de vooraf bepaalde beoordelingscriteria en de programma's die deze criteria toepassen, werken, zodat hij met volledige kennis van zaken kan beslissen of hij zijn recht op beroep al dan niet zal uitoefenen. Zo ook moeten in het kader van een dergelijk beroep de rechter die nagaat of de bevoegde autoriteiten een rechtmatige beslissing hebben genomen en, behalve bij bedreigingen voor de staatsveiligheid, de betrokkene zelf kennis kunnen nemen van de redenen waarom deze beslissing is genomen en van de bewijzen waarop zij steunt, inclusief de vooraf bepaalde beoordelingscriteria en de werking van de programma's die deze criteria toepassen.

- PNR-gegevens kunnen slechts achteraf – dat wil zeggen na de aankomst of het vertrek van de betrokken persoon – worden meegedeeld en beoordeeld indien op grond van nieuwe omstandigheden en objectieve elementen ofwel redelijkerwijs kan worden vermoed dat die persoon betrokken is bij ernstige criminaliteit die minstens indirect een objectief verband vertoont met het luchtvervoer van passagiers, ofwel kan worden aangenomen dat die gegevens in een concreet geval daadwerkelijk terroristische misdrijven die een dergelijk verband vertonen, kunnen helpen bestrijden. Behalve in naar behoren gerechtvaardigde dringende gevallen moeten PNR-gegevens die achteraf ter beoordeling worden meegedeeld in beginsel op gemotiveerd verzoek van de bevoegde autoriteiten eerst worden onderzocht door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit, ongeacht of dit verzoek wordt ingediend vóór dan wel ná het verstrijken van de periode van zes maanden na doorgifte van de gegevens aan de PIE.[21]

Arrest van 22 november 2022 (Grote kamer), Luxembourg Business Registers (C-37/20 en C-601/20, EU:C:2022:912)

De antiwitwasrichtlijn[22] verplicht de lidstaten ter bestrijding en voorkoming van het witwassen van geld en de financiering van terrorisme een register bij te houden dat informatie bevat over de uiteindelijk begunstigden[23] van binnen hun grondgebied opgerichte vennootschappen en andere juridische entiteiten. Na een wijziging van deze richtlijn bij richtlijn 2018/843 [24] moet een deel van die informatie in alle gevallen voor elk lid van de bevolking (hierna: „grote publiek") toegankelijk zijn. Overeenkomstig de aldus gewijzigde antiwitwasrichtlijn (hierna: „gewijzigde antiwitwasrichtlijn") heeft de Luxemburgse wetgever een register van uiteindelijk begunstigden (hierna: „RUB") ingesteld, dat bedoeld is om bepaalde informatie over de uiteindelijk begunstigden van

---

21 Volgens artikel 12, leden 1 en 3, van de PNR-richtlijn is een dergelijke controle slechts uitdrukkelijk voorzien voor verzoeken om mededeling van PNR-gegevens die worden ingediend na de termijn van zes maanden na doorgifte ervan aan de PIE.

22 Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van richtlijn 2005/60/EG van het Europees Parlement en de Raad en richtlijn 2006/70/EG van de Commissie (PB 2015, L 141, blz. 73; hierna: „antiwitwasrichtlijn").

23 Volgens artikel 3, punt 6, van de antiwitwasrichtlijn zijn de uiteindelijk begunstigden de natuurlijke personen die de uiteindelijke eigenaar zijn van of zeggenschap hebben over de cliënt en/of de natuurlijke personen voor wier rekening een transactie of activiteit wordt verricht.

24 Richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de richtlijnen 2009/138/EG en 2013/36/EU (PB 2018, L 156, blz. 43).

geregistreerde entiteiten te bewaren en ter beschikking te stellen. Het RUB is voor iedereen toegankelijk.

In die context hebben WM en Sovim SA bij de Tribunal d'arrondissement de Luxembourg (rechter in eerste aanleg Luxemburg, Luxemburg) elk een zaak aangespannen tegen Luxembourg Business Registers, beheerder van het RUB, omdat die hun verzoeken heeft afgewezen om het grote publiek toegang te weigeren tot informatie die in de eerste zaak betrekking had op WM, als uiteindelijk begunstigde van een vastgoedmaatschappij, en in de tweede zaak op de uiteindelijk begunstigde van Sovim SA. De Tribunal d'arrondissement de Luxembourg heeft twijfels over met name de geldigheid van de Unierechtelijke bepalingen waarbij het stelsel van publieke toegang tot informatie over de uiteindelijk begunstigden is ingevoerd, en heeft daarom het Hof in het kader van die twee zaken een prejudiciële vraag ter beoordeling van de geldigheid gesteld.

In zijn arrest verklaart het Hof (Grote kamer) richtlijn 2018/843 ongeldig voor zover daarbij de antiwitwasrichtlijn in die zin is gewijzigd dat de lidstaten ervoor moeten zorgen dat de informatie over de uiteindelijk begunstigden van op hun grondgebied opgerichte vennootschappen en andere juridische entiteiten in alle gevallen voor het grote publiek toegankelijk is.[25]

In de eerste plaats stelt het Hof vast dat de toegang van het grote publiek tot informatie over de uiteindelijk begunstigden waarin de gewijzigde antiwitwasrichtlijn voorziet, een ernstige inmenging vormt in de grondrechten op eerbiediging van het privéleven en op bescherming van persoonsgegevens, die respectievelijk zijn verankerd in de artikelen 7 en 8 van het Handvest.

Dienaangaande merkt het Hof op dat de betrokken gegevens informatie bevatten over geïdentificeerde natuurlijke personen, namelijk de uiteindelijk begunstigden van vennootschappen en andere juridische entiteiten die binnen het grondgebied van de lidstaten zijn opgericht, zodat de toegang van het grote publiek tot die gegevens raakt aan het grondrecht op bescherming van het privéleven. Bovendien vormt de terbeschikkingstelling ervan aan het grote publiek een verwerking van persoonsgegevens. Het Hof voegt daaraan toe dat deze terbeschikkingstelling aan het grote publiek een inmenging vormt in de twee genoemde grondrechten, ongeacht hoe de meegedeelde informatie later wordt gebruikt.

Wat de ernst van deze inmenging betreft, wijst het Hof erop dat voor zover de aan het grote publiek ter beschikking gestelde informatie betrekking heeft op de identiteit van de uiteindelijk begunstigde en op de aard en omvang van zijn economische belangen in vennootschappen en andere juridische entiteiten, op basis van deze informatie een profiel kan worden opgemaakt met bepaalde persoonlijke identificatiegegevens, de financiële situatie van de betrokkene en de economische sectoren, landen en specifieke ondernemingen waarin hij heeft geïnvesteerd. Bovendien wordt deze informatie voor

---

[25] Ongeldigheid van artikel 1, punt 15, onder c), van richtlijn 2018/843 tot wijziging van artikel 30, lid 5, eerste alinea, onder c), van de antiwitwasrichtlijn.

een potentieel onbeperkt aantal personen toegankelijk, zodat een dergelijke verwerking van persoonsgegevens die informatie ook vrij toegankelijk kan maken voor personen die om redenen die geen verband houden met de door die maatregel nagestreefde doelstelling, informatie wensen te verkrijgen over de situatie van een uiteindelijk begunstigde, in het bijzonder op materieel en financieel gebied. Dit is des te gemakkelijker wanneer de gegevens op internet kunnen worden geraadpleegd. Bovendien worden de mogelijke gevolgen voor de betrokkenen van een eventueel misbruik van hun gegevens nog verergerd doordat deze gegevens, wanneer zij eenmaal ter beschikking van het grote publiek zijn gesteld, niet alleen vrijelijk kunnen worden geraadpleegd, maar ook kunnen worden opgeslagen en verspreid, en het voor deze personen dus nog moeilijker of zelfs nagenoeg onmogelijk wordt om zich doeltreffend tegen misbruik te verdedigen.

In de tweede plaats merkt het Hof in het kader van het onderzoek naar de rechtvaardiging van de betrokken inmenging ten eerste op dat aan het legaliteitsbeginsel is voldaan. De beperking op de uitoefening van bovengenoemde grondrechten als gevolg van de toegang van het grote publiek tot informatie over uiteindelijk begunstigden is namelijk ingevoerd bij een wetgevingshandeling, te weten de gewijzigde antiwitwasrichtlijn. Bovendien vermeldt deze richtlijn dat deze informatie toereikend, accuraat en actueel moet zijn en somt zij uitdrukkelijk bepaalde gegevens op waar het publiek toegang toe moet krijgen. Voorts stelt zij de voorwaarden vast waaronder de lidstaten kunnen voorzien in uitzonderingen op een dergelijke toegang.

Ten tweede maakt het Hof duidelijk dat de betrokken inmenging geen afbreuk doet aan de wezenlijk inhoud van de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten. Hoewel het klopt dat de gewijzigde antiwitwasrichtlijn geen uitputtende lijst bevat de van gegevens waartoe het grote publiek toegang moet krijgen en dat de lidstaten toegang kunnen verlenen tot aanvullende informatie, neemt dit niet weg dat enkel adequate informatie over de uiteindelijk begunstigden en over de door hen gehouden economische belangen kan worden verzameld en bewaard, en bijgevolg eventueel voor het publiek toegankelijk worden gemaakt, hetgeen onder meer informatie uitsluit waarvoor geen toereikend verband met de doelstellingen van de gewijzigde antiwitwasrichtlijn bestaat. De terbeschikkingstelling van informatie aan het grote publiek waarbij een dergelijk verband wel aanwezig is, doet op genigerlei wijze afbreuk aan de wezenlijke inhoud van de bedoelde grondrechten.

Ten derde benadrukt het Hof dat de Uniewetgever, door te voorzien in de toegang van het grote publiek tot informatie over uiteindelijk begunstigden, beoogt het witwassen van geld en de financiering van terrorisme te voorkomen door via een grotere transparantie een omgeving te creëren die minder gemakkelijk daartoe kan worden gebruikt, wat een doelstelling van algemeen belang vormt die zelfs een ernstige inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten kan rechtvaardigen.

Ten vierde stelt het Hof in het kader van de beoordeling van het passende, noodzakelijke en evenredige karakter van de betrokken inmenging vast dat de toegang van het grote publiek tot informatie over de uiteindelijk begunstigden geschikt is om bij te dragen tot de verwezenlijking van deze doelstelling.

Het Hof is evenwel van mening dat deze inmenging niet kan worden geacht beperkt te zijn tot wat strikt noodzakelijk is. Om te beginnen kan niet worden aangetoond dat die inmenging strikt noodzakelijk is op grond van het feit dat het criterium „legitiem belang" – waarover volgens de antiwitwasrichtlijn, in de versie van vóór de wijziging ervan bij richtlijn 2018/843, iedereen die toegang wenste te krijgen tot informatie over de uiteindelijk begunstigden moest beschikken – moeilijk toepasbaar was en dat de toepassing ervan tot willekeurige beslissingen kon leiden. Het feit dat het moeilijk kan zijn om nauwkeurig vast te stellen in welke gevallen en onder welke voorwaarden publieke toegang tot informatie over de uiteindelijk begunstigden mogelijk is, kan niet rechtvaardigen dat de Uniewetgever bepaalt dat het grote publiek toegang heeft tot deze informatie.

Voorts blijkt uit de toelichting in richtlijn 2018/843 evenmin dat de betrokken inmenging strikt noodzakelijk is.[26] Volgens deze toelichting zou publieke toegang tot informatie over uiteindelijk begunstigden meer onderzoek van informatie door de maatschappij, met name door de pers of maatschappelijke organisaties, mogelijk maken, en hebben bijgevolg zowel de pers als de maatschappelijke organisaties die zich bezighouden met de voorkoming en bestrijding van het witwassen van geld en terrorismefinanciering, een legitiem belang bij toegang tot de betrokken informatie. Hetzelfde geldt voor personen die de identiteit van de uiteindelijk begunstigden van een vennootschap of een andere juridische entiteit willen kennen omdat zij mogelijkerwijs transacties met hen zullen aangaan, en voor financiële instellingen en autoriteiten die betrokken zijn bij de bestrijding van delicten op het gebied van het witwassen van geld of terrorismefinanciering.

Daarenboven is de betrokken inmenging evenmin evenredig. Dienaangaande stelt het Hof vast dat de materiële regels die deze inmenging regelen, niet voldoen aan het vereiste van duidelijkheid en nauwkeurigheid. De gewijzigde witwasrichtlijn bepaalt immers dat het grote publiek „ten minste" tot de daarin bedoelde gegevens toegang moet hebben, en verleent de lidstaten de mogelijkheid om toegang te verlenen tot aanvullende informatie, waaronder „ten minste" de geboortedatum of de contactgegevens van de betrokken uiteindelijk begunstigde. Door het gebruik van de uitdrukking „ten minste" maakt deze richtlijn het mogelijk dat gegevens die niet voldoende bepaald of identificeerbaar zijn, aan het publiek beschikbaar worden gesteld.

Wat voorts de afweging tussen de ernst van deze inmenging en het belang van de beoogde doelstelling van algemeen belang betreft, erkent het Hof dat deze doelstelling, gelet op het belang ervan, zelfs een ernstige inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten kan rechtvaardigen.

Niettemin is de bestrijding van het witwassen van geld en van terrorismefinanciering in de eerste plaats een zaak van de overheid en van entiteiten zoals kredietinstellingen of financiële instellingen die uit hoofde van hun activiteiten specifieke verplichtingen op dit gebied hebben. Om die reden bepaalt de gewijzigde witwasrichtlijn dat informatie over

---

[26] Het gaat om de toelichting in overweging 30 van richtlijn 2018/843.

de uiteindelijk begunstigde in alle gevallen toegankelijk moet zijn voor de bevoegde autoriteiten en de financiële-inlichtingeneenheden, zonder enige beperking, en voor de meldingsplichtige entiteiten, in het kader van het cliëntenonderzoek.[27]

Voorts leidt de bij richtlijn 2018/843 ingevoerde regeling, in vergelijking met de vroegere regeling, die naast de toegang van de bevoegde autoriteiten en bepaalde entiteiten tot informatie over uiteindelijk begunstigden voorzag in de toegang van elke persoon of organisatie die een legitiem belang kon aantonen, tot een aanzienlijk zwaardere aantasting van de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten, zonder dat dit kan worden gecompenseerd door de eventuele voordelen die deze laatste regeling ten opzichte van de eerste regeling zou kunnen bieden op het gebied van de strijd tegen het witwassen van geld en terrorismefinanciering.

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)

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 elektronischecommunicatiediensten 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 namelijk de aanbieders van elektronischecommunicatiediensten om alle verkeersgegevens en locatiegegevens van alle abonnees en geregistreerde gebruikers betreffende alle elektronischecommunicatiemiddelen stelselmatig en voortdurend te bewaren, zonder enige uitzondering. 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.

---

[27] Artikel 30, lid 5, eerste alinea, onder a) en b), van de gewijzigde witwasrichtlijn.

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 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 elektronischecommunicatiemiddelen. 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, van richtlijn 2002/58, gelezen tegen de achtergrond van voornoemde artikelen van het Handvest, vereist.

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.

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 beantwoorden 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 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.

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

1. Werkingssfeer van de algemene regelgeving

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 wellicht in strijd waren 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[28] 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[29] 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

---

[28] 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).

[29] 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).

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.

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.

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.

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 beschikking en dus een verwerking van gegevens die buiten de werkingssfeer van de richtlijn viel. Bijgevolg heeft het Hof het besluit van de Raad houdende goedkeuring van de sluiting van de overeenkomst nietig verklaard.

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 van 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 zou worden 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 hij dat Google Spain of Google zou worden gelast zijn persoonsgegevens te verwijderen of te maskeren, zodat deze uit de zoekresultaten en uit de koppelingen van La Vanguardia Ediciones zouden verdwijnen.

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 bevolen de nodige maatregelen te nemen om de gegevens uit hun index te verwijderen en de toegang daartoe in de toekomst 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.

In dat arrest heeft het Hof zich eveneens 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.

In dergelijke omstandigheden zijn de activiteiten van de exploitant van de zoekmachine en die van zijn in de betrokken lidstaat gevestigde vestiging, hoewel zij losstaan van elkaar, immers onlosmakelijk met elkaar verbonden, daar de activiteiten inzake de advertentieruimte het middel vormen om de betrokken zoekmachine economisch rendabel te maken en deze machine tegelijkertijd het middel is waardoor deze activiteiten kunnen worden verricht.

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.

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 tegen de achtergrond van de grondrechten die in het Handvest zijn opgenomen, dient de uitzondering waarin is voorzien in artikel 3, lid 2, tweede streepje, van die richtlijn, strikt te worden uitgelegd. 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.

Arrest van 16 januari 2024 (Grote kamer), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

Omdat er sprake was van mogelijke politieke beïnvloeding van het Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (federaal bureau voor de bescherming van de grondwet en de bestrijding van terrorisme, Oostenrijk)[30] heeft de Nationalrat (lagerhuis van het parlement, Oostenrijk) een enquêtecommissie (hierna: BVT-enquêtecommissie) ingesteld om dit na te gaan. Deze commissie heeft WK als getuige gehoord. Hoewel WK om anonimiteit had verzocht, werd het verslag van zijn hoorzitting

[30] Op 1 december 2021 is deze instantie de Direktion Staatsschutz und Nachrichtendienst (directoraat staatsveiligheid en inlichtingendienst, Oostenrijk) geworden.

gepubliceerd op de website van het Parlament Österreich (Oostenrijks parlement), met vermelding van zijn volledige voor- en achternaam. WK voerde aan dat de openbaarmaking van zijn identiteit in strijd was met de AVG en met Oostenrijks recht en heeft een klacht ingediend bij de Österreichische Datenschutzbehörde (toezichthoudende autoriteit op het gebied van gegevensbescherming, Oostenrijk; hierna: „Datenschutzbehörde"). Bij besluit van 18 september 2019 heeft de Datenschutzbehörde zich onbevoegd verklaard om uitspraak te doen over de klacht omdat het op grond van het beginsel van de scheiding der machten uitgesloten is dat zij, als orgaan van de uitvoerende macht, toezicht houdt op de BVT-enquêtecommissie, die onderdeel is van de wetgevende macht.

Nadat het Bundesverwaltungsgericht (federale bestuursrechter in eerste aanleg, Oostenrijk) het door WK ingestelde beroep had toegewezen en het besluit van de Datenschutzbehörde nietig had verklaard, heeft de Datenschutzbehörde tegen het vonnis van het Bundesverwaltungsgericht beroep in Revision ingesteld bij de hoogste bestuursrechter.

Tegen deze achtergrond heeft de verwijzende rechter het Hof de vraag gesteld of de activiteiten van een enquêtecommissie die door het parlement van een lidstaat is ingesteld, binnen de werkingssfeer van de AVG vallen en of deze verordening van toepassing is wanneer deze activiteiten de bescherming van de nationale veiligheid betreffen.

In de eerste plaats merkt het Hof op dat artikel 2, lid 2, onder a), AVG, waarin wordt bepaald dat deze verordening niet van toepassing is op de verwerking van persoonsgegevens in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen, enkel tot doel heeft om de verwerking door overheidsinstanties in het kader van activiteiten die ertoe strekken de nationale veiligheid te beschermen of die in dezelfde categorie kunnen worden ondergebracht, van de werkingssfeer van die verordening uit te sluiten. Dat het gaat om specifieke activiteiten van de staat of een overheidsinstantie, is dus op zichzelf niet voldoende om automatisch uit te sluiten dat de AVG van toepassing op die activiteiten.

Deze uitlegging, die voortvloeit uit het feit dat de AVG geen onderscheid maakt naargelang van wie de betrokken verwerking verricht, wordt bevestigd door artikel 4, punt 7, AVG[31].

Het Hof wijst erop dat de parlementaire aard van de BVT-enquêtecommissie niet impliceert dat haar activiteiten van het toepassingsgebied van de AVG zijn uitgesloten. De in artikel 2, lid 2, onder a), van deze verordening neergelegde uitzondering heeft immers slechts betrekking op categorieën activiteiten die naar hun aard niet binnen de werkingssfeer van het Unierecht vallen en niet op categorieën personen. Bijgevolg kan op basis van het feit dat de verwerking van persoonsgegevens wordt verricht door een

[31] Dit artikel definieert het begrip „verwerkingsverantwoordelijke" als „een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt".

enquêtecommissie die door het parlement van een lidstaat is ingesteld ter uitoefening van zijn recht van toezicht op de uitvoerende macht, als zodanig niet worden geoordeeld dat deze verwerking plaatsvindt in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen.

In de tweede plaats merkt het Hof op dat het weliswaar aan de lidstaten staat om hun wezenlijke veiligheidsbelangen te definiëren en passende maatregelen te nemen teneinde de veiligheid te verzekeren[32], maar dat het enkele feit dat een nationale maatregel is genomen met het oog op de bescherming van de nationale veiligheid er niet toe kan leiden dat het Unierecht niet van toepassing is en dat de lidstaten worden ontheven van de verplichting om dit recht te eerbiedigen. De uitzondering van artikel 2, lid 2, onder a), AVG heeft slechts betrekking op categorieën activiteiten die naar hun aard niet binnen de werkingssfeer van het Unierecht vallen. Het is op zichzelf niet voldoende dat de verwerkingsverantwoordelijke een overheidsinstantie is waarvan de hoofdactiviteiten bestaan in het waarborgen van de nationale veiligheid, om de verwerking van persoonsgegevens die deze instantie in het kader van haar andere activiteiten verricht uit te sluiten van de werkingssfeer van de AVG.

In casu lijkt er bij het door de BVT-enquêtecommissie uitgeoefende politieke toezicht als zodanig geen sprake te zijn van activiteiten waarmee de nationale veiligheid wordt beschermd of die in die categorie kunnen worden ondergebracht. Deze activiteiten vallen, onder voorbehoud van verificatie door de verwijzende rechter, dus niet buiten de werkingssfeer van de AVG.

Een parlementaire enquêtecommissie kan echter toegang hebben tot persoonsgegevens die om redenen van nationale veiligheid bijzondere bescherming behoeven. In dit verband kunnen er door middel van een wetgevingsmaatregel beperkingen aan de uit de AVG voortvloeiende verplichtingen en rechten worden gesteld, onder meer om de nationale veiligheid te waarborgen.[33] Op deze basis kan het dus gerechtvaardigd zijn dat er beperkingen worden gesteld met betrekking tot het verzamelen van persoonsgegevens, de aan de betrokkenen te verstrekken informatie en hun toegang tot die gegevens of de openbaarmaking ervan – zonder toestemming van de betrokkenen – aan andere personen dan de verwerkingsverantwoordelijke, op voorwaarde dat die beperkingen de wezenlijke inhoud van de grondrechten en fundamentele vrijheden van de betrokkenen onverlet laten en in een democratische samenleving een noodzakelijke en evenredige maatregel zijn.

Het Hof wijst er evenwel op dat uit de informatie waarover het beschikt, niet blijkt dat de BVT-enquêtecommissie heeft gesteld dat de openbaarmaking van de persoonsgegevens van de betrokkene noodzakelijk was om de nationale veiligheid te waarborgen en gebaseerd was op een daartoe vastgestelde nationale wetgevingsmaatregel, hetgeen indien nodig door de verwijzende rechter moet worden geverifieerd.

---

32 Overeenkomstig artikel 4, lid 2, VEU.

33 Volgens artikel 23 AVG.

2. Begrip „persoonsgegevens”

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

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 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 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.

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.

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 is het zo dat indien de examinator de identiteit van de kandidaat niet kent op het moment van de beoordeling van de door de kandidaat verstrekte examenantwoorden, de instantie die het examen organiseert – in casu de beroepsorganisatie van accountants – wel degelijk over de nodige informatie beschikt die deze instantie in staat stelt 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 waar het om een openboekexamen gaat.

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.

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 inzonderheid hun nauwkeurigheid en de noodzaak om te worden bewaard in de zin van artikel 6, lid 1, onder d) en e), van richtlijn 95/46, alsook kunnen worden gerectificeerd of gewist uit hoofde van artikel 12, onder b), van de 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 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.

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.

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 in 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. Een dergelijke verwerking van persoonsgegevens die geschiedt met het oog op het verrichten van vrijwilligerswerk of religieuze activiteiten, valt immers onder geen 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.

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

In dit arrest (zie ook rubriek II.1, „Werkingssfeer van de algemene regeling"), heeft het Hof de gelegenheid gehad 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. 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 gekwalificeerd. Een algemene afwijking van de toepassing van de richtlijn in een dergelijke hypothese zou deze richtlijn grotendeels zinloos maken.

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

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 namelijk 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 en zijn deze richtsnoeren terug te vinden in ten minste één van de aan de verkondigingsactiviteit gewijde tijdschriften van deze gemeenschap.

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.

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[34] 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.

De verwijzende rechter heeft geoordeeld dat hij 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 oordeelt het Hof (Grote kamer) dat de verwerking van persoonsgegevens die betrekking hebben op strafpunten een „verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten"[35] is, waarvoor de AVG meer bescherming biedt omdat de gegevens in kwestie bijzonder gevoelig zijn.

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

---

[34] Artikel 14[1], lid 2, van de Ceļu satiksmes likums (wet betreffende het wegverkeer) van 1 oktober 1997 (Latvijas Vēstnesis, 1997, nr. 274/276).
[35] Artikel 10 AVG.

werkingssfeer van deze verordening is namelijk zeer ruim en die verwerking valt niet onder de uitzonderingen op de toepasselijkheid van die verordening.

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.[36] 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.

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.[37] Het Hof stelt namelijk vast dat de CSDD bij het verstrekken van die gegevens niet kan worden aangemerkt als een „bevoegde autoriteit” in die zin.[38]

Voorts onderzoekt het Hof of de toegang tot persoonsgegevens betreffende verkeersovertredingen, zoals strafpunten, een verwerking vormt van persoonsgegevens betreffende „strafbare feiten”[39], die een ruimere bescherming genieten. In dit verband constateert het Hof dat dit begrip uitsluitend betrekking heeft op strafbare feiten in strafrechtelijke zin. 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 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

---

36 Artikel 2, lid 2, onder a), AVG.

37 Artikel 2, lid 2, onder d), AVG.

38 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).

39 Artikel 10 AVG.

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 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.

Arrest van 5 december 2023 (Grote kamer), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

In 2020 hebben de Litouwse autoriteiten met het oog op een betere beheersing van de COVID-19-pandemie besloten om een mobiele IT-applicatie aan te schaffen. Deze app moest helpen bij de epidemiologische follow-up door het registreren en monitoren van gegevens over mensen die waren blootgesteld aan het COVID-19-virus.

Daartoe heeft de Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (nationaal centrum voor volksgezondheid van het ministerie van Volksgezondheid, Litouwen; hierna: „NVSC”), dat verantwoordelijk was voor de aanschaf van deze app, contact opgenomen met de vennootschap UAB „IT sprendimai sėkmei” (hierna: „ITSS”), met het verzoek om een dergelijke mobiele app te ontwikkelen. Vervolgens hebben de werknemers van het NVSC aan deze vennootschap e-mails gezonden waarin zij met name uitlegden welke vragen er in deze app moesten worden gesteld.

In de periode van april tot en met mei 2020 stond de door ITSS ontwikkelde mobiele app ter beschikking van het publiek. Als gevolg daarvan hebben 3 802 personen van deze app gebruikgemaakt en verschillende gegevens over zichzelf verstrekt, zoals gevraagd in deze app. Wegens een gebrek aan financiering heeft het NVSC aan ITSS echter geen overheidsopdracht voor de officiële aankoop van haar mobiele app gegund en de desbetreffende procedure beëindigd.

Ondertussen had de nationale toezichthoudende autoriteit een onderzoek ingesteld naar de verwerking van persoonsgegevens als gevolg van het gebruik van deze app. Bij besluit van deze autoriteit, dat is vastgesteld na afloop van het onderzoek, zijn er administratieve geldboeten opgelegd aan zowel het NVSC als ITSS, die als gezamenlijke verwerkingsverantwoordelijke werden beschouwd.

Het NVSC is tegen dit besluit opgekomen bij de Vilniaus apygardos administracinis teismas (bestuursrechter in eerste aanleg Vilnius, Litouwen). Aangezien deze rechter twijfels had over de uitlegging van verschillende bepalingen van de AVG, heeft hij het Hof om een prejudiciële beslissing verzocht.

In zijn arrest verduidelijkt het Hof (Grote kamer) onder meer het begrip „verwerking”. Dienaangaande verklaart het dat het gebruik van persoonsgegevens in het kader van IT-tests van een mobiele app een verwerking vormt in de zin van de AVG. Dit is echter niet

het geval indien die gegevens zodanig zijn geanonimiseerd dat de persoon op wie die gegevens betrekking hebben niet of niet meer identificeerbaar is of wanneer het gaat om fictieve gegevens die geen betrekking hebben op een bestaande natuurlijke persoon.

De vraag of persoonsgegevens worden gebruikt voor IT-tests dan wel voor een ander doel is namelijk irrelevant voor de kwalificatie van de handeling als „verwerking". Verder kan alleen een verwerking die betrekking heeft op „persoonsgegevens" worden gekwalificeerd als een „verwerking" in de zin van de AVG. Fictieve of anonieme gegevens zijn evenwel geen persoonsgegevens.

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, „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. Om onder dit begrip te vallen hoeft een dergelijk geheel geen steekkaarten, specifieke lijsten of andere ordeningssystemen te omvatten.

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, „Begrip ‚verwerking van persoonsgegevens'" en II.4, „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.

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

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 „voor de verwerking van persoonsgegevens verantwoordelijke” nader bepaald. Het Hof heeft in dit verband vastgesteld dat de beheerder van een fanpagina op Facebook, 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.

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 deze zaak 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 vindt kennelijk plaats zonder

dat die bezoeker zich daarvan bewust is en ongeacht of hij al dan niet lid is van het sociaal netwerk Facebook of op de vind-ik-leukknop van Facebook heeft geklikt.

De Verbraucherzentrale NRW, een Duitse vereniging van algemeen nut die consumentenbelangen behartigt, verwijt 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).

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.

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.

Arrest van 5 december 2023 (Grote kamer), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

In deze zaak (zie tevens rubriek I.3 „Begrip ‚verwerking van persoonsgegevens’”) merkt het Hof op dat een entiteit die een onderneming opdracht heeft gegeven om een mobiele IT-applicatie te ontwikkelen en in die context heeft deelgenomen aan de

vaststelling van het doel van en de middelen voor de verwerking van persoonsgegevens via die app, als verwerkingsverantwoordelijke kan worden beschouwd.[40] Die vaststelling blijft ook overeind indien die entiteit niet zelf persoonsgegevens heeft verwerkt, niet uitdrukkelijk heeft ingestemd met de uitvoering van de specifieke handelingen voor die verwerking of voor de beschikbaarstelling van de mobiele app aan het publiek, en zij deze app niet heeft aangekocht, tenzij die entiteit zich vóór die beschikbaarstelling aan het publiek uitdrukkelijk heeft verzet tegen de beschikbaarstelling en de verwerking van de persoonsgegevens als gevolg daarvan.

6. Begrip „gezamenlijke verwerkingsverantwoordelijke”

Arrest van 5 december 2023 (Grote kamer), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

In deze zaak (zie tevens de rubrieken I.3, „Begrip ‚verwerking van persoonsgegevens’” en I.5, „Begrip ‚voor de verwerking van persoonsgegevens verantwoordelijke’”) wijst het Hof erop dat het, om twee entiteiten als gezamenlijke verwerkingsverantwoordelijken te kunnen kwalificeren, niet nodig is dat er tussen deze entiteiten een regeling bestaat over de vaststelling van het doel van en de middelen voor de verwerking van de persoonsgegevens, of dat er een regeling bestaat waarin de voorwaarden betreffende de gezamenlijke verantwoordelijkheid voor de verwerking worden vastgesteld. Het is juist dat de gezamenlijke verwerkingsverantwoordelijken krachtens de AVG[41] hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze verordening op transparante wijze dienen vast te stellen door middel van een onderlinge regeling. Het bestaan van een dergelijke regeling vormt echter geen voorafgaande voorwaarde om twee of meer entiteiten als „gezamenlijke verwerkingsverantwoordelijken” te kwalificeren, maar een verplichting die de AVG oplegt aan de gezamenlijke verwerkingsverantwoordelijken, zodra zij als verwerkingsverantwoordelijken zijn gekwalificeerd, teneinde de naleving van de uit hoofde van de AVG op hen rustende verplichtingen te verzekeren. Deze kwalificatie vloeit dus voort uit het enkele feit dat meerdere entiteiten hebben deelgenomen aan de vaststelling van het doel van en de middelen voor de verwerking.

Wat de gezamenlijke vaststelling door de betrokken entiteiten van het doel van en de middelen voor de verwerking betreft, preciseert het Hof dat hun deelname aan die vaststelling verschillende vormen kan aannemen en het resultaat kan zijn zowel van hun gezamenlijk besluit als van hun convergerende besluiten. In dit laatste geval moeten de besluiten elkaar aanvullen, zodat elk ervan een concreet effect heeft op de vaststelling van het doel van en de middelen voor de verwerking.

---

40 In de zin van artikel 4, punt 7, AVG.

41 Artikel 26, lid 1, AVG, gelezen in het licht van overweging 79 van die verordening.

7. Voorwaarden voor een rechtmatige verwerking van persoonsgegevens

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

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.

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 Oberverwaltungsgericht für das Land Nordrhein-Westfalen (hoogste bestuursrechter van de deelstaat Noordrijn-Westfalen, Duitsland), waar het geschil aanhangig werd gemaakt, het Hof gevraagd of de verwerking van persoonsgegevens in dit register 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.

Wat het begrip „noodzakelijk” zijn 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 de uitvoering van de bepalingen ervan 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.

Voorts heeft het Hof met betrekking tot het gebruik van de in het register opgenomen gegevens voor de criminaliteitsbestrijding met name opgemerkt dat deze is gericht 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.

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

In dit arrest (zie tevens rubriek II.2, „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 deze zaak had de Duitse regeling echter de mogelijkheid om bepaalde categorieën persoonsgegevens te verwerken categorisch en generiek uitgesloten, zonder dat in een bepaald geval een afweging kan worden gemaakt aan de hand van de rechten en belangen die in een concreet geval over en weer op het spel staan. 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.

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 lijsten 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.

In dit verband heeft het Hof opgemerkt dat het aan de nationale rechter staat 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.

Voorts heeft het Hof vastgesteld dat wanneer een persoon op de litigieuze lijst is ingeschreven, dat bepaalde van zijn rechten kan 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.

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.

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

Orange România levert mobieletelecommunicatiediensten 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 mobiele telecommunicatiediensten gesloten die een beding 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[42] voorziet in een lijst van gevallen waarin een verwerking van persoonsgegevens als rechtmatig kan worden aangemerkt. In het bijzonder moet de toestemming van de betrokkene vrij, specifiek,

---

[42] Artikel 7 van richtlijn 95/46 en artikel 6 AVG.

geïnformeerd en ondubbelzinnig worden gegeven.[43] In dit verband wordt de toestemming niet rechtsgeldig gegeven in geval van stilzwijgen, reeds aangekruiste vakjes of inactiviteit.

Indien de betrokkene toestemming geeft in het kader van een schriftelijke verklaring die ook op andere aangelegenheden betrekking heeft, moet die verklaring 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.

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 nationale rechter om de daartoe vereiste controles te verrichten.

Volgens het Hof dient deze rechter eveneens 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, ingeval deze geen toestemming gaf om zijn gegevens te verwerken, eiste dat deze schriftelijk verklaart 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 van hen niet eisen dat zij actief blijk geven van hun weigering.

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 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

---

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

verantwoordelijke doordat geëist wordt dat de betrokkene, om uiting te geven aan zijn weigering toestemming te geven, een aanvullend formulier invult waaruit die weigering blijkt.

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 waarbij aan de Ceļu satiksmes drošības direkcija (directie verkeersveiligheid, Letland) (hierna: „CSDD") de verplichting wordt opgelegd om gegevens die betrekking hebben op strafpunten die aan bestuurders van voertuigen zijn toegekend wegens verkeersovertredingen, toegankelijk te maken voor het publiek, zonder dat degene die om toegang verzoekt hoeft aan te tonen dat hij een specifiek belang heeft bij het verkrijgen van die gegevens. Volgens het Hof is er 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 de regeling in kwestie rechtvaardigen.

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"[44]. Vast staat evenwel niet 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.

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

---

[44] 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".

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

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.

III. Verwerking van persoonsgegevens in de zin van de sectorale regeling

1. Verwerking van persoonsgegevens in de sector elektronische communicatie

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

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 elektronischecommunicatiediensten 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, 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 elektronischecommunicatiediensten 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.

In deze context heeft het Hof gepreciseerd dat het in het arrest Tele2 Sverige en Watson e.a.[45] weliswaar had geoordeeld dat alleen de bestrijding van zware criminaliteit kan rechtvaardigen dat overheidsinstanties toegang krijgen tot door aanbieders van elektronischecommunicatiediensten 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.

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.

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

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 aan aanbieders van elektronischecommunicatiediensten geen verplichting tot algemene en

---

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

ongedifferentieerde verplichting tot bewaring van verkeers- en locatiegegevens kunnen opleggen, heeft geleid tot bezorgdheid bij bepaalde staten, die vrezen dat hun een instrument is ontnomen dat zij noodzakelijk achten om de nationale veiligheid te waarborgen en criminaliteit te bestrijden.

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 (hoogste bestuursrechter, 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 die terreinen vastgestelde regelingen die met name voorzien in een verplichting voor aanbieders van elektronischecommunicatiediensten 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 heeft het Hof (Grote kamer) allereerst geoordeeld dat nationale regelingen waarbij ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een verplichting tot bewaring van verkeers- en locatiegegevens dan wel tot doorzending van deze gegevens aan de veiligheids- en inlichtingendiensten wordt opgelegd, binnen de werkingssfeer van richtlijn 2002/58 vallen.

Vervolgens brengt het Hof in herinnering dat richtlijn 2002/58 [46] niet toestaat dat de uitzondering op de principeverplichting om de vertrouwelijkheid van elektronische communicatie en van de daarmee verband houdende gegevens te waarborgen, en op het verbod om deze gegevens op te slaan, de regel wordt. Dit impliceert dat deze richtlijn de lidstaten slechts toestaat om, onder meer ten behoeve van de nationale veiligheid, wettelijke maatregelen te treffen ter beperking van de omvang van de erin bedoelde rechten en plichten, met name de verplichting om de vertrouwelijkheid van elektronische communicatie en van de daarmee verband houdende gegevens[47] te waarborgen, 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[48].

In dit verband komt het Hof in de zaak Privacy International tot het oordeel 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 elektronischecommunicatiediensten 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

---

46 Artikel 15, leden 1 en 3, van richtlijn 2002/58.
47 Artikel 5, lid 1, van richtlijn 2002/58.
48 Met name de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest.

aanbieders van elektronischecommunicatiediensten 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 van wie de gegevens aan de orde zijn, een verband vertoont met de doelstelling die door de betrokken regeling wordt nagestreefd. Het Hof geeft een vergelijkbare uitlegging aan artikel 23, lid 1, AVG, gelezen in het licht van het Handvest, dat zich naar zijn oordeel verzet tegen een nationale regeling waarbij aan 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.

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 elektronischecommunicatiediensten 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, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin is voorzien. In diezelfde omstandigheden verzet genoemde richtlijn zich evenmin tegen een geautomatiseerde analyse van met name de verkeers- en locatiegegevens van alle gebruikers van elektronischecommunicatiemiddelen.

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 elektronischecommunicatiemiddelen, 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, wanneer die feiten of verstoringen reeds zijn vastgesteld dan wel wanneer er een redelijke verdenking bestaat dat dergelijke feiten zijn gepleegd of dat de nationale veiligheid wordt bedreigd.

Voorts oordeelt het Hof dat richtlijn 2002/58, gelezen in het licht van het Handvest, zich niet verzet tegen een nationale regeling die aanbieders van elektronischecommunicatiediensten ertoe 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 de een of andere manier betrokken zijn bij terroristische activiteiten, en is onderworpen aan voorafgaande toetsing door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is en die zich ervan vergewist dat een dergelijke maatregel slechts wordt toegestaan binnen de grenzen van het strikt noodzakelijke. In urgente gevallen dient die toetsing op korte termijn plaats te vinden.

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 is het van oordeel 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 elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens wordt opgelegd die als onverenigbaar is aangemerkt met richtlijn 2002/58, gelezen in het licht van het Handvest.

Om de verwijzende rechter een nuttig antwoord te verstrekken, roept het Hof in herinnering dat de aanvaarding en de beoordeling van bewijzen die door middel van een met het Unierecht strijdige gegevensbewaring zijn verkregen 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 is van het nationale recht. 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.

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[49].

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 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 betwijfelt de verwijzende rechter 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.[50] die de met het onderzoek belaste instantie toegang kan verlenen tot de betrokken gegevens.

In zijn arrest, dat door de Grote kamer is gewezen, oordeelt het Hof dat richtlijn 2002/58, gelezen in het licht van het Handvest, zich verzet tegen een nationale regeling op grond waarvan overheidsinstanties met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten toegang kunnen krijgen tot 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, zonder dat die toegang beperkt is tot procedures ter bestrijding van zware criminaliteit of ter voorkoming van ernstige bedreigingen van de openbare veiligheid. Volgens het Hof is 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 samenhang met 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.

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

---

[49] 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.
[50] Arrest van 21 december 2016, Tele2 Sverige en Watson e.a. (C-203/15 en C-698/15, *EU:C:2016:970*, punt 120).

kunnen hebben dat de doelstelling van voorkoming, onderzoek, opsporing en vervolging van strafbare feiten in het algemeen een dergelijke toegang rechtvaardigt.

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 elektronischecommunicatiediensten 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 beschermd tegen het risico van misbruik. Die regeling moet wettelijk verbindend zijn naar nationaal recht en in het bijzonder 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.

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.

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.

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, enerzijds niet betrokken mag zijn bij de uitvoering van het betrokken strafrechtelijk onderzoek en, anderzijds, neutraal moet zijn ten opzichte van de partijen in de strafprocedure. Dat is niet het geval bij een openbaar ministerie, zoals het Estse parket, dat de onderzoeksprocedure leidt en, in voorkomend geval, optreedt als openbaar aanklager. Hieruit volgt dat het openbaar ministerie niet in een positie is om de bovengenoemde voorafgaande toetsing te verrichten.

Arrest van 5 april 2022 (Grote kamer), Commissioner of An Garda Síochána e.a. (C-140/20, EU:C:2022:258)

In deze zaak heeft de Supreme Court (hoogste rechterlijke instantie, Ierland) een verzoek om een prejudiciële beslissing ingediend in het kader van een civiele procedure die is ingesteld door een persoon die tot een levenslange gevangenisstraf is veroordeeld wegens een in Ierland begane moord. Die persoon betwist daarin de verenigbaarheid met het Unierecht van enkele bepalingen van de nationale wet inzake de bewaring van in het kader van elektronische communicatie gegenereerde gegevens. Aanbieders van elektronische-communicatiediensten hebben overeenkomstig deze wet verkeers- en locatiegegevens van telefoongesprekken van de beklaagde bewaard en vrijgegeven aan de politie. De verwijzende rechter heeft er in het bijzonder twijfels over of een systeem waarbij deze gegevens algemeen en ongedifferentieerd worden bewaard ter bestrijding van zware criminaliteit, wel verenigbaar is met richtlijn 2002/58, gelezen in het licht van het Handvest.

In zijn arrest bevestigt het Hof (Grote kamer) de rechtspraak die voortvloeit uit het arrest La Quadrature du Net e.a.[51] en verduidelijkt het de draagwijdte ervan. Het herinnert eraan dat verkeers- en locatiegegevens van elektronische communicatie niet algemeen en ongedifferentieerd mogen worden bewaard ter bestrijding van zware criminaliteit en ter voorkoming van ernstige bedreigingen voor de openbare veiligheid. Het bevestigt ook de rechtspraak uit het arrest Prokuratuur (Voorwaarden voor toegang tot elektronische-communicatiegegevens)[52], met name de regel dat de toegang van de bevoegde nationale autoriteiten tot die bewaarde gegevens vooraf moet worden getoetst door ofwel een rechterlijke instantie ofwel een van een politiefunctionaris onafhankelijke bestuurlijke entiteit.

In de eerste plaats oordeelt het Hof dat richtlijn 2002/58, gelezen in het licht van het Handvest, zich verzet tegen wettelijke maatregelen die met het oog op de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens. Gelet op het ontmoedigende effect dat de bewaring van die gegevens kan hebben op de uitoefening van de grondrechten[53], en de ernst van de

---

51 Arrest van 6 oktober 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 en C-520/18, *EU:C:2020:791*).

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

53 Verankerd in de artikelen 7 tot en met 11 van het Handvest.

inmenging die een dergelijke bewaring met zich brengt, moet deze bewaring immers de uitzondering en niet de regel zijn in het bij richtlijn 2002/58 ingevoerde stelsel, zodat de betrokken gegevens niet stelselmatig en continu kunnen worden bewaard. Zelfs zeer zware criminaliteit kan niet worden gelijkgesteld met een bedreiging voor de nationale veiligheid, aangezien met een dergelijke gelijkstelling een intermediaire categorie tussen nationale en openbare veiligheid zou kunnen worden gecreëerd om vervolgens op die laatste categorie de vereisten toe te passen die inherent zijn aan de eerste.

Richtlijn 2002/58, gelezen in het licht van het Handvest, verzet zich daarentegen niet tegen wettelijke maatregelen die met het oog op de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een gerichte bewaring van verkeers- en locatiegegevens die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van categorieën betrokken personen of van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd. Het Hof voegt daaraan toe dat de bevoegde autoriteiten met een dergelijke bewaringsmaatregel voor plekken of faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht of voor strategische plekken, zoals vliegvelden, stations, zeehavens of tolzones, informatie kunnen verkrijgen over de aanwezigheid op die plekken van personen die daar een elektronische-communicatiemiddel gebruiken, en daaruit met het oog op de bestrijding van zware criminaliteit conclusies kunnen trekken over hun aanwezigheid en activiteiten op die plekken. Dat het eventueel moeilijk is om nauwkeurig vast te stellen in welke gevallen en onder welke voorwaarden voor gerichte bewaring moet worden gekozen, kan hoe dan ook niet rechtvaardigen dat de lidstaten tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens overgaan.

Die richtlijn, gelezen in het licht van het Handvest, verzet zich evenmin tegen wettelijke maatregelen die om diezelfde redenen voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk, en van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische-communicatiemiddelen. Wat dit laatste aspect betreft, preciseert het Hof in het bijzonder dat noch richtlijn 2002/58 noch enige andere handeling van Unierecht zich verzet tegen nationale wetgeving die tot doel heeft zware criminaliteit te bestrijden en die de toekenning van een elektronische-communicatiemiddel, zoals een vooraf betaalde simkaart, afhankelijk stelt van de verificatie van officiële documenten waaruit de identiteit van de koper blijkt, en van de registratie van de daarin vervatte informatie door de verkoper, waarbij die verkoper in voorkomend geval gehouden is de bevoegde nationale autoriteiten toegang tot deze informatie te geven.

Hetzelfde geldt voor wettelijke maatregelen die ter bestrijding van zware criminaliteit en ter voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in de mogelijkheid om via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronische-communicatiediensten een bevel op te leggen tot spoedbewaring (*quick freeze*) van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode. Een dergelijke bewaring kan immers enkel worden gerechtvaardigd door de bestrijding van zware criminaliteit en, a fortiori, de bescherming van de openbare veiligheid, op voorwaarde dat de

maatregel en de toegang tot de bewaarde gegevens worden beperkt tot het strikt noodzakelijke. Het Hof brengt in herinnering dat een dergelijke spoedbewaringsmaatregel kan worden uitgebreid tot verkeers- en locatiegegevens van andere personen dan die welke ervan worden verdacht een ernstig strafbaar feit of handelingen die een gevaar voor de nationale veiligheid vormen te hebben voorbereid of gepleegd, op voorwaarde dat op basis van objectieve en niet-discriminatoire factoren kan worden geoordeeld dat die gegevens kunnen helpen bij het ophelderen van een dergelijk strafbaar feit of een dergelijke verstoring van de nationale veiligheid. In dit verband kan bijvoorbeeld worden gedacht aan de gegevens van het slachtoffer van het strafbare feit of van personen uit zijn sociale of werkomgeving.

Het Hof geeft vervolgens evenwel aan dat alle voormelde wettelijke maatregelen, door het gebruik van duidelijke en nauwkeurige regels, moeten verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik. De verschillende bewaringsmaatregelen voor verkeers- en locatiegegevens kunnen naar keuze van de nationale wetgever en binnen de grenzen van het strikt noodzakelijke tegelijkertijd worden toegepast.

Voorts verduidelijkt het Hof dat het zou indruisen tegen de hiërarchie van doelstellingen van algemeen belang die een maatregel uit hoofde van richtlijn 2002/58 kunnen rechtvaardigen, om in de strijd tegen zware criminaliteit toegang te verlenen tot gegevens die algemeen en ongedifferentieerd zijn bewaard om het hoofd te bieden aan een ernstige bedreiging voor de nationale veiligheid. Dit zou er immers op neerkomen dat de toegang kan worden gerechtvaardigd met een minder belangrijke doelstelling dan die welke de bewaring rechtvaardigde – de bescherming van de nationale veiligheid –, waardoor het verbod om die gegevens in de strijd tegen zware criminaliteit algemeen en ongedifferentieerd te bewaren, elke nuttige werking zou dreigen te verliezen.

In de tweede plaats oordeelt het Hof dat richtlijn 2002/58, gelezen in het licht van het Handvest, zich verzet tegen nationale wetgeving op grond waarvan de gecentraliseerde behandeling van verzoeken om toegang tot door aanbieders van elektronische-communicatiediensten bewaarde gegevens die de politie tijdens het onderzoek naar en de vervolging van ernstige strafbare feiten indient, is opgedragen aan een politiefunctionaris, zelfs al wordt hij bijgestaan door een binnen de politie opgerichte eenheid die een zekere mate van autonomie heeft bij de uitvoering van haar taak en waarvan de beslissingen later door een rechter kunnen worden getoetst. Een dergelijke politiefunctionaris voldoet immers niet aan de vereisten van onafhankelijkheid en onpartijdigheid die gelden voor een bestuurlijke autoriteit die door de bevoegde nationale autoriteiten ingediende verzoeken om toegang tot gegevens vooraf toetst, aangezien hij niet de hoedanigheid van derde ten opzichte van deze autoriteiten heeft. Bovendien kan de beslissing van een dergelijke functionaris weliswaar a posteriori worden getoetst door een rechter, maar kan deze toetsing niet in de plaats komen van een onafhankelijke toetsing die, behalve in naar behoren gemotiveerde urgente gevallen, op voorhand gebeurt.

In de derde plaats, ten slotte, bevestigt het Hof zijn rechtspraak dat het Unierecht zich ertegen verzet dat een nationale rechter de werking in de tijd beperkt van de ongeldigverklaring van nationale wetgeving die aanbieders van elektronische-communicatiediensten een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens oplegt, die hij op grond van het nationale recht dient uit te spreken wegens de onverenigbaarheid van die wetgeving met richtlijn 2002/58. Het Hof herinnert er wel aan dat de toelaatbaarheid van de via die bewaring verkregen bewijzen een kwestie is die overeenkomstig het beginsel van de procedurele autonomie van de lidstaten onder het nationale recht valt, op voorwaarde dat met name de beginselen van gelijkwaardigheid en doeltreffendheid worden geëerbiedigd.

Arrest van 20 september 2022 (Grote kamer), VD en SR (C-339/20 en C-397/20, EU:C:2022:703)

Na een onderzoek van de Autorité des marchés financiers (autoriteit voor financiële markten, Frankrijk; AMF) zijn tegen VD en SR, twee natuurlijke personen, strafprocedures ingesteld wegens handel met voorkennis, heling van handel met voorkennis, medeplichtigheid, omkoping en witwassen. De AMF had in het kader van dat onderzoek persoonsgegevens uit telefoongesprekken van VD en SR gebruikt die op grond van de code des postes et des communications électroniques (wetboek posterijen en elektronische communicatie) waren verkregen in het kader van de levering van elektronischecommunicatiediensten.

Voor zover hun respectieve inbeschuldigingstelling steunde op de door de AMF verstrekte verkeersgegevens hebben VD en SR elk beroep ingesteld bij de cour d'appel de Paris (rechter in tweede aanleg Parijs, Frankrijk). Zij hebben daarbij met name schending aangevoerd van 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. Zij hebben zich in het bijzonder gebaseerd op de rechtspraak van het arrest Tele2 Sverige en Watson e.a.[54] en bezwaar gemaakt tegen het feit dat de AMF zich voor het verzamelen van die gegevens had beroepen op de betrokken nationale bepalingen, hoewel deze bepalingen volgens hen, ten eerste, niet in overeenstemming waren met het Unierecht, voor zover zij voorzagen in een algemene en ongedifferentieerde bewaring van de verkeersgegevens en, ten tweede, geen enkele limiet stelden aan de bevoegdheid van de AMF-onderzoekers om de bewaarde gegevens op te vragen.

Bij twee arresten van 20 december 2018 en 7 maart 2019 heeft de cour d'appel de Paris de beroepen van VD en SR verworpen. De feitenrechters hebben zich voor de afwijzing van voormeld middel met name gebaseerd op het feit dat de verordening betreffende marktmisbruik[55] de bevoegde autoriteit de mogelijkheid biedt om, voor zover dat door de nationale wetgeving is toegestaan, bestaande verkeersgegevensoverzichten te vorderen waarover een operator van elektronischecommunicatiediensten beschikt,

---

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

[55] Verordening (EU) nr. 596/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende marktmisbruik (verordening marktmisbruik) en houdende intrekking van richtlijn 2003/6 en richtlijnen 2003/124/EG, 2003/125/EG en 2004/72/EG van de Commissie (PB 2014, L 173, blz. 1).

wanneer er een redelijk vermoeden van een inbreuk op het verbod op handel met voorwetenschap bestaat en dergelijke overzichten relevant kunnen zijn voor het onderzoek naar deze inbreuk.

VD en SR hebben daarop cassatieberoep ingesteld bij de Cour de cassation (hoogste rechter in burgerlijke en strafzaken, Frankrijk), de verwijzende rechter in de onderhavige zaken.

In deze context vraagt die rechter zich af hoe artikel 15, lid 1, van richtlijn 2002/58, gelezen tegen de achtergrond van het Handvest, moet worden verzoend met de vereisten van artikel 12, lid 2, onder a) en d), van de richtlijn „marktmisbruik”[56] en artikel 23, lid 2, onder g) en h), van de verordening betreffende marktmisbruik. Meer bepaald gaat het in deze zaak over nationale wettelijke maatregelen die operatoren van elektronischecommunicatiediensten in de strijd tegen marktmisbruik – waarvan handel met voorkennis deel uitmaakt – preventief verplichten om verkeersgegevens algemeen en ongedifferentieerd te bewaren gedurende een jaar vanaf de datum van registratie. Voor het geval het Hof van oordeel zou zijn dat de in het hoofdgeding aan de orde zijnde wetgeving over de bewaring van verbindingsgegevens niet verenigbaar is met het Unierecht, vraagt de verwijzende rechter zich af of de gevolgen van deze wetgeving voorlopig in stand kunnen worden gehouden, teneinde rechtsonzekerheid te vermijden en het mogelijk te maken om de eerder verzamelde en bewaarde gegevens te gebruiken voor de opsporing en vervolging van handel met voorwetenschap.

Het Hof (Grote kamer) komt in zijn arrest tot het oordeel dat het operatoren van elektronischecommunicatiediensten niet is toegestaan om in de strijd tegen marktmisbruik verkeersgegevens preventief algemeen en ongedifferentieerd te bewaren gedurende een jaar vanaf de datum van registratie. Verder bevestigt het zijn rechtspraak dat het Unierecht zich ertegen verzet dat een nationale rechter de werking in de tijd beperkt van de ongeldigverklaring van nationale wettelijke bepalingen die hij dient uit te spreken wegens de onverenigbaarheid ervan met het Unierecht.

Het Hof herinnert er om te beginnen aan dat bij de uitlegging van een bepaling van Unierecht niet alleen rekening moet worden gehouden met de bewoordingen ervan, maar ook met de context ervan en de doelstellingen van de regeling waarvan zij deel uitmaakt.

Wat de bewoordingen van de in de prejudiciële vragen vermelde bepalingen betreft, constateert het Hof dat daar waar artikel 12, lid 2, onder d), van de richtlijn „marktmisbruik” spreekt van de bevoegdheid van de AMF om „bestaande overzichten van telefoon- en dataverkeer te vereisen”, artikel 23, lid 2, onder g) en h), van de verordening betreffende marktmisbruik het heeft over de bevoegdheid van die autoriteit om „overzichten van dataverkeer waarover beleggingsondernemingen, kredietinstellingen of financiële instellingen […] beschikken” en „voor zover dat door de nationale wetgeving is toegestaan, […] bestaande verkeersgegevensoverzichten

---

[56] Richtlijn 2003/6/EG van het Europees Parlement en de Raad van 28 januari 2003 betreffende handel met voorwetenschap en marktmanipulatie (marktmisbruik) (PB 2003, L 96, blz. 16).

waarover een telecommunicatie-exploitant beschikt” te vorderen. Volgens het Hof blijkt uit de tekst van deze bepalingen duidelijk dat deze enkel de bevoegdheid van de AMF regelen om de gegevens waarover die operatoren beschikken te „vereisen” of te „vorderen”, wat overeenkomt met toegang tot die gegevens. Voorts suggereert de verwijzing naar „bestaande” overzichten „waarover [die operatoren] beschikken”, dat de Uniewetgever niet de bedoeling heeft gehad om regels te geven voor de mogelijkheid voor de nationale wetgever om een bewaarplicht voor die overzichten in te voeren. Deze uitlegging vindt volgens het Hof steun zowel in de context van die bepalingen als in de doelstellingen van de regeling waarvan die bepalingen deel uitmaken.

Wat de context van de in de prejudiciële vragen genoemde bepalingen betreft, merkt het Hof op dat de Uniewetgever volgens de relevante bepalingen van de richtlijn „marktmisbruik” en de verordening betreffende marktmisbruik[57] de lidstaten weliswaar heeft willen verplichten de nodige maatregelen te nemen om ervoor te zorgen dat de voor financiën bevoegde autoriteiten over een geheel van passende instrumenten, bevoegdheden en middelen beschikken alsook over de nodige toezichts- en onderzoeksbevoegdheden om de doeltreffendheid van hun taken te waarborgen, maar dat deze bepalingen niets zeggen over de eventuele mogelijkheid van de lidstaten om daartoe voor de operatoren van elektronischecommunicatiediensten een algemene en ongedifferentieerde bewaarplicht van verkeersgegevens in te voeren, noch over de condities waarin de operatoren die gegevens moeten bewaren met het oog op de eventuele overlegging ervan aan de bevoegde autoriteiten.

Wat de doelstellingen van de betrokken regeling betreft, merkt het Hof op dat uit de richtlijn „marktmisbruik” en de verordening betreffende marktmisbruik[58] blijkt dat deze instrumenten tot doel hebben de integriteit van de financiële markten van de Unie te waarborgen en het vertrouwen van de beleggers in deze markten te vergroten, welk vertrouwen onder meer berust op de omstandigheid dat zij met elkaar op voet van gelijkheid verkeren en dat zij zullen worden beschermd tegen het ongeoorloofde gebruik van voorwetenschap. Derhalve heeft het bij deze instrumenten ingestelde verbod op handel met voorwetenschap[59] tot doel de gelijkheid van de partijen bij een beurstransactie te waarborgen door te vermijden dat een van de contractanten die over voorwetenschap beschikt en bijgevolg een voordeel heeft ten opzichte van de andere investeerders, hiervan profiteert ten nadele van de anderen, die hiervan niet op de hoogte zijn. Hoewel overzichten van verbindingsgegevens volgens de verordening betreffende marktmisbruik[60] cruciaal bewijs en soms het enige bewijs vormen waarmee handel met voorwetenschap of marktmanipulatie aan het licht kan worden gebracht en kan worden bewezen, neemt dit niet weg dat deze verordening enkel spreekt van overzichten „waarover [operatoren van elektronischecommunicatiediensten] beschikken” en van de bevoegdheid van de voor financiën bevoegde autoriteit om

---

57 Respectievelijk artikel 12, lid 1, van de richtlijn „marktmisbruik” en artikel 23, lid 3, van de verordening betreffende marktmisbruik, gelezen in het licht van overweging 62 van deze verordening.

58 Respectievelijk de overwegingen 2 en 12 van de richtlijn „marktmisbruik” en artikel 1 van de verordening betreffende marktmisbruik, gelezen in het licht van de overwegingen 2 en 24 van deze verordening.

59 Artikel 2, lid 1, van de richtlijn „marktmisbruik” en artikel 8, lid 1, van de verordening betreffende marktmisbruik.

60 Overweging 62 van de verordening betreffende marktmisbruik.

„bestaande” gegevens bij die operatoren „op te vragen”. Uit deze tekst blijkt dus nergens dat de Uniewetgever met deze verordening de lidstaten de bevoegdheid heeft willen geven om operatoren van elektronischecommunicatiediensten een algemene bewaarplicht voor deze gegevens op te leggen. Bijgevolg kan noch de richtlijn „marktmisbruik” noch de verordening betreffende marktmisbruik, met het oog op de uitoefening van de bevoegdheden die de voor financiën bevoegde autoriteit aan deze handelingen ontleent, de rechtsgrond vormen voor een algemene bewaarplicht voor verkeersgegevensoverzichten waarover operatoren van elektronischecommunicatiediensten beschikken.

Vervolgens brengt het Hof in herinnering dat de richtlijn 2002/58 de referentiehandeling vormt op het gebied van bewaring en meer algemeen verwerking van persoonsgegevens in de sector elektronische communicatie, zodat de aan deze richtlijn gegeven uitlegging ook moet gelden voor verkeersgegevensoverzichten waarover operatoren van elektronischecommunicatiediensten beschikken en die de voor financiën bevoegde autoriteiten in de zin van de richtlijn „marktmisbruik” en de verordening betreffende marktmisbruik[61] bij hen kunnen opvragen. Bijgevolg moet de rechtmatigheid van de verwerking van de overzichten waarover de operatoren van elektronischecommunicatiediensten beschikken[62], worden beoordeeld aan de hand van de voorwaarden in richtlijn 2002/58 en van de uitlegging van deze richtlijn in de rechtspraak van het Hof.

Aldus oordeelt het Hof dat de richtlijn „marktmisbruik” en de verordening betreffende marktmisbruik, gelezen in samenhang met richtlijn 2002/58 en tegen de achtergrond van het Handvest, zich verzetten tegen wettelijke maatregelen die ter bestrijding van marktmisbruik, waarvan handel met voorwetenschap deel uitmaakt, operatoren van elektronischecommunicatiediensten verplichten verkeersgegevens preventief tijdelijk (namelijk gedurende een jaar vanaf de datum van registratie), maar algemeen en ongedifferentieerd te bewaren.

Tot slot bevestigt het Hof zijn rechtspraak dat het Unierecht zich ertegen verzet dat een nationale rechter de werking in de tijd beperkt van de ongeldigverklaring van nationale bepalingen die operatoren van elektronischecommunicatiediensten verplichten om verkeersgegevens algemeen en ongedifferentieerd te bewaren en die toestaan dat die gegevens worden meegedeeld aan de voor financiën bevoegde autoriteit zonder voorafgaande goedkeuring van een rechter of een onafhankelijke administratieve autoriteit, welke ongeldigverklaring hij op grond van het nationale recht dient uit te spreken wegens de onverenigbaarheid van die bepalingen met richtlijn 2002/58, gelezen tegen de achtergrond van het Handvest. Het Hof brengt evenwel in herinnering dat de toelaatbaarheid van de via die bewaring verkregen bewijzen een kwestie is die overeenkomstig het beginsel van de procedurele autonomie van de lidstaten onder het nationale recht valt, op voorwaarde dat met name de beginselen van gelijkwaardigheid en doeltreffendheid worden geëerbiedigd. Dit laatste beginsel brengt voor de nationale

---

61 Respectievelijk artikel 11 van de richtlijn „marktmisbruik” en artikel 22 van de verordening betreffende marktmisbruik.

62 In de zin van artikel 12, lid 2, onder d), van de richtlijn „marktmisbruik” en artikel 23, lid 2, onder g) en h), van de verordening betreffende marktmisbruik.

strafrechter de verplichting mee om informatie en bewijzen die door middel van een met het Unierecht onverenigbare algemene en ongedifferentieerde bewaring zijn verkregen, buiten beschouwing te laten indien de betrokken personen niet in de gelegenheid zijn om doeltreffend commentaar te leveren op die informatie en die bewijzen, en deze betrekking hebben op een gebied waarvan de rechter geen kennis heeft en van doorslaggevende invloed kunnen zijn op de beoordeling van de feiten.

Arrest van 30 april 2024 (voltallige zitting), La Quadrature du Net e.a. (Persoonsgegevens en bestrijding van namaak) (C-470/21, EU:C:2024:370)

Naar aanleiding van een verzoek van de Conseil d'État (hoogste bestuursrechter, Frankrijk) om een prejudiciële beslissing vult de voltallige zitting van het Hof zijn rechtspraak over richtlijn 2002/58 aan met preciseringen over, ten eerste, de voorwaarden waaronder een algemene bewaring van IP-adressen door aanbieders van elektronischecommunicatiediensten niet kan worden geacht te leiden tot een ernstige inmenging in de door het Handvest gewaarborgde rechten op eerbiediging van het privéleven, bescherming van persoonsgegevens en vrijheid van meningsuiting[63], en, ten tweede, de mogelijkheid voor een overheidsinstantie om, in het kader van de bestrijding van online gepleegde inbreuken op intellectuele-eigendomsrechten, toegang te krijgen tot bepaalde persoonsgegevens die met inachtneming van dergelijke voorwaarden worden bewaard.

In deze zaak hebben vier verenigingen bij de Premier ministre (eerste minister, Frankrijk) een verzoek ingediend tot intrekking van het décret relatif au traitement automatisé de données à caractère personnel (decreet betreffende de geautomatiseerde verwerking van persoonsgegevens)[64]. Aangezien aan dit verzoek geen gevolg is gegeven, hebben deze verenigingen bij de Conseil d'État beroep tot nietigverklaring van deze stilzwijgende afwijzing ingesteld. Volgens hen zijn dit decreet en de bepalingen die de rechtsgrondslag ervan vormen[65], in strijd met het Unierecht.

Krachtens de Franse wetgeving heeft de Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet [hoge autoriteit voor de verspreiding van werken en de bescherming van rechten op het internet (Hadopi)], teneinde de personen te kunnen identificeren die verantwoordelijk zijn voor online gepleegde inbreuken op auteursrechten of naburige rechten, toegang tot bepaalde gegevens die de aanbieders van elektronische-communicatiediensten moeten bewaren. Deze gegevens hebben betrekking op de burgerlijke identiteit van de betrokken personen die overeenkomt met

---

63 De artikelen 7, 8 en 11 van het Handvest.

64 Décret no 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé „Système de gestion des mesures pour la protection des œuvres sur internet" [decreet nr. 2010-236 van 5 maart 2010 betreffende de geautomatiseerde verwerking van persoonsgegevens die bekendstaat onder de benaming „Systeem voor het beheer van maatregelen voor de bescherming van werken op het internet" en die wordt toegestaan door artikel L. 331-29 van het wetboek voor intellectuele eigendom (hierna: „CPI"); JORF nr. 56 van 7 maart 2010, tekst nr. 19], zoals gewijzigd bij décret no 2017-924, du 6 mai 2017, relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (decreet nr. 2017-924 van 6 mei 2017 betreffende het beheer van auteursrechten en naburige rechten door een instantie voor het beheer van rechten en tot wijziging van het CPI; JORF nr. 109 van 10 mei 2017, tekst nr. 176).

65 Met name artikel L. 331-21, derde tot en met vijfde alinea, van de code de la propriété intellectuelle.

hun IP-adressen die vooraf door organisaties van rechthebbenden zijn verzameld. Zodra de houder van het IP-adres dat wordt gebruikt voor activiteiten die een dergelijke inbreuk opleveren, is geïdentificeerd, volgt Hadopi de zogenoemde „graduated response”-procedure. In concreto is deze autoriteit bevoegd om aan deze houder twee aanbevelingen te verzenden, die zijn te vergelijken met waarschuwingen, en, indien de activiteiten voortduren, een kennisgevingsbrief waarin hem wordt meegedeeld dat zijn activiteiten strafrechtelijk kunnen worden vervolgd. Ten slotte kan zij zich tot het openbaar ministerie wenden met het oog op de vervolging van de betrokkene.[66]

In deze context heeft de Conseil d’État het Hof verzocht om uitlegging van richtlijn 2002/58, gelezen in het licht van het Handvest.[67]

Wat in de eerste plaats de bewaring van gegevens betreffende de burgerlijke identiteit en van de overeenkomstige IP-adressen betreft, benadrukt het Hof dat niet elke algemene en ongedifferentieerde bewaring van IP-adressen noodzakelijkerwijs een ernstige inmenging vormt in de door het Handvest gewaarborgde rechten op eerbiediging van het privéleven, op bescherming van persoonsgegevens en op vrijheid van meningsuiting.

De verplichting om voor een dergelijke bewaring te zorgen kan worden gerechtvaardigd door de doelstelling van bestrijding van strafbare feiten in het algemeen, wanneer daadwerkelijk is uitgesloten dat die bewaring kan leiden tot ernstige inmenging in het privéleven van de betrokkene doordat daarover nauwkeurige gevolgtrekkingen kunnen worden gemaakt, onder meer door die IP-adressen te koppelen aan een verzameling verkeers- of locatiegegevens.

Bijgevolg moet een lidstaat die aan aanbieders van elektronischecommunicatiediensten een dergelijke verplichting wil opleggen, zich ervan vergewissen dat die gegevens zodanig worden bewaard dat het is uitgesloten dat nauwkeurige gevolgtrekkingen over het privéleven van de betrokkenen kunnen worden gemaakt.

Het Hof verduidelijkt dat daartoe de wijzen van bewaring betrekking moet hebben op de structuur zelf van de bewaring, die in wezen zodanig moet worden ingericht dat een daadwerkelijk volledige scheiding van de verschillende categorieën bewaarde gegevens wordt gegarandeerd., d doordat een beveiligd en betrouwbaar IT-instrument wordt gebruikt. Zo moeten de nationale regels voor de wijze van bewaring De nationale regels die betrekking hebben op die bewaarwijzen moeten dus garanderen dat elke categorie gegevens, met inbegrip van de gegevens betreffende de burgerlijke identiteit en de IP-adressen, volledig gescheiden van de andere categorieën bewaarde gegevens wordt bewaard en dat deze scheiding daadwerkelijk volledig is, doordat een beveiligd en betrouwbaar IT-instrument wordt gebruikt. Bovendien mogen die regels, voor zover zij voorzien in de mogelijkheid om de bewaarde IP-adressen te koppelen aan de burgerlijke identiteit van de betrokkene met het oog op de bestrijding van inbreuken, een dergelijke

---

66 Met ingang van 1 januari 2022 is Hadopi gefuseerd met de Conseil supérieur de l’audiovisuel [hoge raad voor de audiovisuele sector (CSA)], een andere onafhankelijke overheidsinstantie, tot de Autorité de régulation de la communication audiovisuelle et numérique [regelgevende instantie voor audiovisuele en digitale communicatie (ARCOM)]. De graduated response-procedure is echter in wezen ongewijzigd gebleven.

67 Artikel 15, lid 1, van richtlijn 2002/58.

koppeling slechts mogelijk maken met behulp van een efficiënt technisch procedé dat geen afbreuk doet aan de doeltreffendheid van de volledige scheiding van deze categorieën gegevens. De betrouwbaarheid van deze scheiding moet regelmatig worden getoetst door een derde overheidsinstantie. Voor zover in de toepasselijke nationale wetgeving is voorzien in dergelijke strikte vereisten, kan de uit deze bewaring van IP-adressen voortvloeiende inmenging niet als „ernstig" worden aangemerkt.

Het Hof oordeelt dan ook dat, wanneer er sprake is van wetgeving die gegarandeerd uitsluit dat er door gegevens te koppelen nauwkeurige gevolgtrekkingen kunnen worden gemaakt over het privéleven van de personen wier gegevens worden bewaard, richtlijn 2002/58, gelezen in het licht van het Handvest, zich er niet tegen verzet dat een lidstaat voor een periode die niet langer is dan strikt noodzakelijk een verplichting tot algemene en ongedifferentieerde bewaring van IP-adressen oplegt met het oog op de bestrijding van strafbare feiten in het algemeen.

Wat in de tweede plaats de toegang tot met IP-adressen overeenkomende gegevens betreffende de burgerlijke identiteit betreft, verklaart het Hof voor recht dat richtlijn 2002/58, gelezen in het licht van het Handvest, zich in beginsel niet verzet tegen een nationale regeling waarbij aan een overheidsinstantie toegang wordt verleend tot deze gegevens die daadwerkelijk volledig gescheiden worden bewaard door aanbieders van elektronische-communicatiediensten, met als enige doel dat deze instantie de houders van deze adressen die ervan worden verdacht verantwoordelijk te zijn voor op het internet gepleegde inbreuken op de auteursrechten en naburige rechten, kan identificeren en tegen hen kan optreden. In een dergelijk geval moet de nationale regeling de ambtenaren die over die toegang beschikken, verbieden om, ten eerste, informatie over de inhoud van de door die houders geraadpleegde bestanden in welke vorm ook openbaar te maken – tenzij dit gebeurt om de feiten ter kennis van het openbaar ministerie te brengen – , ten tweede, de zoekgeschiedenis van die houders te traceren en, ten derde, deze IP-adressen te gebruiken voor andere doeleinden dan de vaststelling van die maatregelen.

In dit verband herinnert het Hof er met name aan dat, ook al zijn de vrijheid van meningsuiting en de vertrouwelijkheid van persoonsgegevens belangrijke prioriteiten, deze grondrechten niet absoluut zijn. Bij een afweging van de betrokken rechten en belangen moeten deze grondrechten namelijk soms wijken voor andere grondrechten en vereisten van algemeen belang, zoals de bescherming van de openbare orde en het voorkomen van strafbare feiten of de bescherming van de rechten en vrijheden van anderen. Dit is met name het geval wanneer het doorslaggevende belang dat aan die prioriteiten wordt gehecht, de doeltreffendheid van een vooronderzoek kan belemmeren, met name doordat het onmogelijk of uiterst moeilijk wordt om de dader van een strafbaar feit daadwerkelijk te identificeren en hem een sanctie op te leggen.

Eveneens in dit verband verwijst het Hof tevens naar zijn rechtspraak volgens welke, waar het de bestrijding van online gepleegde strafbare feiten die inbreuk maken op auteursrechten of naburige rechten betreft, de omstandigheid dat de toegang tot IP-adressen het enige onderzoeksmiddel kan zijn met behulp waarvan de betrokkene kan worden geïdentificeerd, lijkt aan te tonen dat de bewaring van en de toegang tot die adressen strikt noodzakelijk zijn om het nagestreefde doel te bereiken en dus voldoen

aan het vereiste van evenredigheid. Indien een dergelijke toegang niet zou worden verleend, zou overigens een reëel risico van systematische straffeloosheid ontstaan voor strafbare feiten die online worden gepleegd of waarvan het plegen of voorbereiden wordt vergemakkelijkt door de specifieke kenmerken van het internet. Het bestaan van een dergelijk risico vormt een relevante omstandigheid wanneer in het kader van een afweging van de verschillende betrokken rechten en belangen wordt beoordeeld of een inmenging in het recht op eerbiediging van het privéleven, het recht op bescherming van persoonsgegevens en op vrijheid van meningsuiting een maatregel is die evenredig is aan het doel van bestrijding van strafbare feiten.

In de derde plaats oordeelt het Hof, wat betreft de vraag of de toegang van de overheidsinstantie tot met een IP-adres overeenkomende gegevens betreffende de burgerlijke identiteit afhankelijk moet worden gesteld van een voorafgaande toetsing door een rechterlijke instantie of een onafhankelijke bestuurlijke entiteit, dat een dergelijke toetsing vereist is wanneer die toegang, in de context van een nationale regeling, het risico inhoudt van een ernstige inmenging in de grondrechten van de betrokkene, in die zin dat die overheidsinstantie op basis daarvan nauwkeurige gevolgtrekkingen over zijn privéleven kan maken en, in voorkomend geval, een gedetailleerd profiel van hem kan bepalen. Omgekeerd is het niet de bedoeling dat dit vereiste van voorafgaande toetsing wordt toegepast wanneer de inmenging in de grondrechten niet als ernstig kan worden aangemerkt.

In dit verband preciseert het Hof dat er, wanneer er een bewaringsmechanisme wordt ingesteld dat daadwerkelijk volledige scheiding van deze verschillende categorieën gegevens waarborgt, in beginsel geen voorafgaande toetsing voor de toegang van de overheidsinstantie tot de met de IP-adressen overeenkomende gegevens betreffende de burgerlijke identiteit vereist is. Een dergelijke toegang met als enig doel de houder van een IP-adres te identificeren, vormt in de regel namelijk geen ernstige inmenging in bovengenoemde rechten.

Het Hof sluit evenwel niet uit dat er in atypische situaties een risico bestaat dat de overheidsinstantie in het kader van een procedure als de in het hoofdgeding aan de orde zijnde graduated response-procedure nauwkeurige gevolgtrekkingen over het privéleven van een persoon kan maken, met name wanneer de betrokkene zich herhaaldelijk of zelfs op grote schaal bezighoudt met activiteiten die inbreuk maken op auteursrechten of naburige rechten op peer-to-peernetwerken, in verband met specifieke soorten beschermde werken die – in voorkomend geval gevoelige – informatie over aspecten van zijn privéleven onthullen.

In casu kan een houder van een IP-adres met name worden blootgesteld aan een dergelijk risico wanneer de overheidsinstantie moet beslissen om de feiten al dan niet aan het openbaar ministerie te melden met het oog op zijn vervolging. De intensiteit van de inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer kan namelijk toenemen naarmate de graduated response-procedure, die een bepaalde volgorde aanhoudt, de verschillende fasen ervan doorloopt. Doordat de bevoegde autoriteit toegang heeft tot de reeks gegevens over de betrokkene die in de verschillende fasen van die procedure zijn verzameld, is zij mogelijk in staat om nauwkeurige gevolgtrekkingen te maken over zijn privéleven. Bijgevolg moet de nationale regeling

voorzien in een voorafgaande toetsing, die moet plaatsvinden voordat de overheidsinstantie gegevens betreffende de burgerlijke identiteit kan koppelen aan een dergelijke reeks gegevens, en voordat zij eventueel de kennisgevingsbrief verzendt waarbij wordt vastgesteld dat deze persoon zich schuldig heeft gemaakt aan strafrechtelijk vervolgbare feiten. Deze toetsing moet bovendien de doeltreffendheid van de graduated response-procedure waarborgen, in het bijzonder door het mogelijk te maken de gevallen aan te wijzen waarin het betrokken inbreukmakende gedrag mogelijk opnieuw wordt herhaald. Daartoe moet deze procedure zodanig worden georganiseerd en gestructureerd dat de gegevens betreffende de burgerlijke identiteit van een persoon die overeenkomen met eerder op het internet verzamelde IP-adressen, door de personen die binnen de bevoegde overheidsinstantie belast zijn met het onderzoek van de feiten niet automatisch kunnen worden gekoppeld aan de gegevens waarover deze laatste reeds beschikt en die het mogelijk kunnen maken nauwkeurige gevolgtrekkingen over het privéleven van die persoon te maken.

Wat het voorwerp van de voorafgaande toetsing betreft, merkt het Hof voorts op dat, in de gevallen waarin de betrokkene ervan wordt verdacht een inbreuk te hebben gepleegd die onder strafbare feiten in het algemeen valt, de rechterlijke instantie of de onafhankelijke bestuurlijke entiteit die met die toetsing belast is, de toegang moet weigeren wanneer de overheidsinstantie daardoor in staat zou zijn nauwkeurige gevolgtrekkingen te maken over het privéleven van die persoon. Daarentegen zou zelfs een toegang aan de hand waarvan dergelijke nauwkeurige gevolgtrekkingen kunnen worden gemaakt, moeten worden toegestaan in de gevallen waarin de betrokkene ervan wordt verdacht strafbare feiten te hebben gepleegd die door de betrokken lidstaat als aantasting van een fundamenteel belang van de samenleving worden beschouwd en daardoor als ernstige vorm van criminaliteit kunnen worden aangemerkt.

Het Hof verduidelijkt tevens dat een voorafgaande toetsing in geen geval volledig geautomatiseerd kan zijn, aangezien een dergelijke toetsing in het geval van een strafrechtelijk onderzoek vereist dat de legitieme belangen die verband houden met de bestrijding van criminaliteit worden afgewogen tegen de eerbiediging van de persoonlijke levenssfeer en de bescherming van de persoonsgegevens. Deze afweging vereist de tussenkomst van een natuurlijke persoon, die des te meer noodzakelijk is omdat het automatische karakter en de grote schaal van de betrokken gegevensverwerking risico's voor de persoonlijke levenssfeer met zich meebrengen.

Het Hof komt aldus tot de slotsom dat de mogelijkheid voor de personen die binnen de overheidsinstantie met het onderzoek van de feiten belast zijn, om met een IP-adres overeenkomende gegevens betreffende de burgerlijke identiteit van een persoon te koppelen aan de bestanden die gegevens bevatten aan de hand waarvan de titels kunnen worden achterhaald van de beschermde werken waarvan de terbeschikkingstelling op internet het verzamelen van IP-adressen door organisaties van rechthebbenden heeft gerechtvaardigd, wanneer dezelfde persoon opnieuw een inbreuk op auteursrechten of naburige rechten herhaalt, moet worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke entiteit. Die toetsing kan niet volledig geautomatiseerd zijn en moet plaatsvinden vóór een dergelijke koppeling, die het in zulke gevallen mogelijk kan maken dat er nauwkeurige gevolgtrekkingen worden

gemaakt over het privéleven van die persoon, wiens IP-adres is gebruikt voor activiteiten die inbreuk kunnen maken op auteursrechten of naburige rechten.

In de vierde plaats, ten slotte, merkt het Hof op dat het door de overheidsinstantie gebruikte systeem voor gegevensverwerking op gezette tijden moet worden getoetst door een onafhankelijk orgaan dat ten opzichte van die instantie de hoedanigheid van derde heeft. Deze toetsing heeft tot doel de integriteit van het systeem te verifiëren, met inbegrip van de daadwerkelijke waarborgen tegen het risico van misbruik en tegen onrechtmatige toegang tot en onrechtmatig gebruik van die gegevens, alsmede de doeltreffendheid en betrouwbaarheid ervan voor het opsporen van eventuele tekortkomingen.

In dit verband merkt het Hof op dat in casu de geautomatiseerde verwerking van persoonsgegevens door de overheidsinstantie – op basis van informatie over door de organisaties van rechthebbenden geconstateerde namaak – een bepaald aantal vals-positieve gevallen kan bevatten en vooral het risico met zich meebrengt dat een mogelijk zeer groot aantal gegevens door derden wordt misbruikt of onrechtmatig wordt gebruikt, hetgeen de noodzaak van een dergelijke toetsing verklaart. Voorts merkt het Hof op dat voor deze verwerking de specifieke regels ter bescherming van persoonsgegevens gelden waarin is voorzien in richtlijn 2016/680. In casu beschikt de overheidsinstantie namelijk weliswaar niet over eigen beslissingsbevoegdheden in het kader van de zogenoemde graduated response-procedure, maar moet zij worden aangemerkt als een „overheidsinstantie" die betrokken is bij de voorkoming en de opsporing van strafbare feiten, waardoor zij binnen de werkingssfeer van deze richtlijn valt. De personen op wie een dergelijke procedure betrekking heeft, genieten dan ook een door richtlijn 2016/680 voorgeschreven reeks materiële en procedurele waarborgen en het staat aan de verwijzende rechter om na te gaan of de nationale wetgeving daarin voorziet.

2. Verwerking van persoonsgegevens in strafzaken

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, een 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 is verankerd in zowel artikel 54 van de Overeenkomst ter uitvoering van het Schengenakkoord[68] als artikel 50 van het Handvest – verbiedt met name dat een reeds bij onherroepelijk vonnis berechte persoon opnieuw wordt vervolgd wegens hetzelfde strafbare feit.

In 2017 heeft WS bij het Verwaltungsgericht Wiesbaden (bestuursrechter in eerste aanleg 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 strijd is met richtlijn 2016/680 betreffende de bescherming van persoonsgegevens in strafzaken[69].

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 zijn arrest (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.

---

[68] 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").

[69] 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).

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.[70] 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.[71] De verwerking van de gegevens in kwestie door de autoriteiten van de lidstaten kan overigens juist onontbeerlijk blijken te zijn om na te gaan of dat beginsel van toepassing is.

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.[72]

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, zodat hij niet meer wegens die feiten kan worden aangehouden. Hieruit volgt dat de betrokkene moet kunnen verzoeken om zijn gegevens te wissen. 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.

***Arrest van 21 juni 2022 (Grote kamer), Ligue des droits humains (C-817/19,* EU:C:2022:491)**

In deze zaak (zie tevens rubriek I.1., „Overeenstemming van het afgeleide Unierecht met het recht op bescherming van persoonsgegevens") verduidelijkt het Hof, na te hebben vastgesteld dat de PNR-richtlijn geldig is, de uitlegging van sommige bepalingen ervan[73].

Ten eerste wijst het Hof erop dat deze richtlijn de doelstellingen die met de verwerking van PNR-gegevens worden nagestreefd, limitatief opsomt. Bijgevolg verzet de richtlijn zich tegen nationale wetgeving volgens welke PNR-gegevens mogen worden verwerkt voor andere doeleinden dan de bestrijding van terroristische misdrijven en ernstige

---

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

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

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

73 Met name artikel 2 („Toepassing van [de richtlijn] op vluchten binnen de EU"), artikel 6 („Verwerking van PNR-gegevens") en artikel 12 („Bewaartermijn van de gegevens en anonimisering") van de PNR-richtlijn.

criminaliteit. Zo gaat nationale wetgeving op grond waarvan PNR-gegevens ook mogen worden verwerkt om toe te zien op activiteiten van inlichtingen- en veiligheidsdiensten, mogelijkerwijs voorbij aan het uitputtende karakter van die opsomming. Evenzo kan het systeem van de PNR-richtlijn niet worden aangewend om grenscontroles te verbeteren en illegale immigratie te bestrijden. PNR-gegevens mogen evenmin worden bewaard in één enkele databank die zowel voor de doeleinden van de PNR-richtlijn als voor andere doeleinden kan worden geraadpleegd.

Ten tweede verduidelijkt het Hof het begrip onafhankelijke nationale instantie die bevoegd is om na te gaan of voldaan is aan de voorwaarden om PNR-gegevens mee te delen, met het oog op een beoordeling achteraf en om hiervoor goedkeuring te geven. De instantie die wordt opgericht om als PIE op te treden, kan niet als een dergelijke instantie worden gezien, aangezien zij niet de hoedanigheid van derde heeft ten opzichte van de instantie die om toegang tot de gegevens verzoekt. Het personeel van de PIE kan immers zijn gedetacheerd uit instanties die om dergelijke toegang kunnen verzoeken, zodat de PIE noodzakelijkerwijs aan deze instanties verbonden lijkt te zijn. Bijgevolg verzet de PNR-richtlijn zich tegen nationale wetgeving volgens welke de instantie die wordt opgericht om als PIE op te treden, ook de hoedanigheid heeft van nationale instantie die bevoegd is om goedkeuring te verlenen voor de mededeling van PNR-gegevens na het verstrijken van de periode van zes maanden na doorgifte ervan aan de PIE.

Ten derde oordeelt het Hof in verband met de bewaartermijn van PNR-gegevens dat artikel 12 van de PNR-richtlijn, gelezen in het licht van de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest, zich verzet tegen nationale wetgeving die een algemene bewaartermijn van vijf jaar voorschrijft die zonder onderscheid geldt voor alle luchtreizigers.

Na de initiële bewaartermijn van zes maanden is het volgens het Hof namelijk niet langer strikt noodzakelijk om PNR-gegevens te bewaren van luchtreizigers voor wie noch uit de voorafgaande beoordeling noch uit eventuele controles tijdens de initiële bewaartermijn van zes maanden noch uit andere omstandigheden is gebleken dat er objectieve aanwijzingen zijn – zoals een geverifieerde positieve overeenstemming tijdens de voorafgaande beoordeling – dat het gevaar bestaat dat zij terroristische misdrijven zullen plegen of zich aan ernstige criminaliteit schuldig zullen maken die minstens indirect een objectief verband vertonen met de door hen genomen vlucht. Daarentegen gaat het feit dat de PNR-gegevens van alle luchtreizigers die onder het systeem van deze richtlijn vallen gedurende de initiële termijn van zes maanden worden bewaard, volgens het Hof in beginsel niet verder dan strikt noodzakelijk is.

Ten vierde gaat het Hof nader in op de vraag of de PNR-richtlijn in de strijd tegen terroristische misdrijven en ernstige criminaliteit eventueel kan worden toegepast op andere soorten passagiersvervoer binnen de Unie. De richtlijn, gelezen in het licht van artikel 3, lid 2, VEU, artikel 67, lid 2, VWEU en artikel 45 van het Handvest, verzet zich tegen een systeem waarbij PNR-gegevens voor alle andere soorten vervoer binnen de Unie worden doorgegeven en verwerkt zonder dat de betrokken lidstaat met een werkelijke en actuele of voorzienbare terroristische dreiging wordt geconfronteerd. In een dergelijke situatie mag het systeem van de PNR-richtlijn, net als voor vluchten

binnen de Unie, enkel worden toegepast op PNR-gegevens voor transportmiddelen die met name bepaalde verbindingen en reisroutes of bepaalde treinstations of zeehavens betreffen waarvoor er aanwijzingen bestaan dat deze toepassing gerechtvaardigd is. Het staat dan aan de betrokken lidstaat om het vervoer te selecteren waarvoor er dergelijke aanwijzingen bestaan en om die toepassing regelmatig te herzien in het licht van wijzigingen in de omstandigheden die deze selectie rechtvaardigden.

IV. Doorgifte van persoonsgegevens naar derde landen

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

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.

Gezien de stand van de ontwikkeling van internet ten tijde van de vaststelling van richtlijn 95/46 en het ontbreken van criteria voor het gebruik van internet in hoofdstuk IV, waartoe artikel 25 behoort, dat een controle door de lidstaten van de doorgiften van persoonsgegevens naar derde landen beoogt te waarborgen en de doorgifte daarvan beoogt te verbieden indien daar geen passend beschermingsniveau wordt geboden, kan niet worden aangenomen dat de gemeenschapswetgever de bedoeling had, het begrip „doorgifte van gegevens naar een derde land" ook te laten gelden voor het plaatsen van gegevens op een internetpagina, zelfs wanneer die gegevens daarmee toegankelijk worden gemaakt voor personen uit derde landen die de technische middelen hebben om zich toegang daartoe te verschaffen.

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

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[74] had vastgesteld dat de Verenigde Staten in het kader van de zogenoemde „veiligehavenregeling" (in het Engels: „safe harbour")[75] , 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 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.

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. 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.

---

[74] 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).

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

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 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.

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. Niet beperkt tot het strikt noodzakelijke is aldus een regeling die algemeen toestaat dat alle persoonsgegevens van alle personen van wie de gegevens vanuit de Unie naar de Verenigde Staten worden doorgegeven, worden bewaard, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het nagestreefde doel en zonder dat wordt voorzien in een objectief criterium ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en van 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. 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.

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, 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 de naam en de contactgegevens van de vliegtuigpassagier(s), onder meer gegevens die nodig zijn voor de reservering, zoals de geplande reisdata en de reisroute, informatie over de reisbiljetten, de groepen van personen die onder hetzelfde boekingsnummer geregistreerd zijn, informatie over de betaalmiddelen of de facturatie, bagage-informatie 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.

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).

In dit verband heeft het Hof geoordeeld dat de betrokken inmengingen weliswaar kunnen worden gerechtvaardigd door een doelstelling van algemeen belang (waarborging 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.

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.

In de derde plaats heeft het Hof vastgesteld dat het in artikel 7 van het Handvest 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.

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

De AVG bepaalt dat de doorgifte van persoonsgegevens naar een derde land in beginsel slechts kan plaatsvinden indien het derde land een passend beschermingsniveau waarborgt. Volgens deze verordening kan de Commissie vaststellen dat een derde land op basis van zijn nationale wetgeving of internationale toezeggingen een passend beschermingsniveau waarborgt.[76] Als er geen adequaatheidsbesluit is genomen, mag een dergelijke doorgifte alleen worden uitgevoerd indien de in de Unie gevestigde gegevensexporteur passende waarborgen biedt die met name kunnen voortvloeien uit de door de Commissie vastgestelde standaardbepalingen inzake gegevensbescherming, en indien de betrokkenen beschikken over afdwingbare rechten en doeltreffende rechtsmiddelen.[77] Verder bepaalt de AVG op nauwkeurige wijze welke voorwaarden gelden voor een dergelijke doorgifte bij het ontbreken van een adequaatheidsbesluit of passende waarborgen.[78]

Maximillian Schrems is een Oostenrijks staatsburger die in Oostenrijk woont en die sinds 2008 Facebook gebruikt. Zoals het geval is bij andere Facebookgebruikers in de Unie, worden de persoonsgegevens van Schrems door Facebook Ireland geheel of gedeeltelijk doorgegeven naar servers van Facebook Inc. in de Verenigde Staten en worden zij daar verwerkt. Schrems heeft bij de Ierse toezichthoudende autoriteit een klacht ingediend en in essentie verzocht om deze doorgiften te verbieden. Hij heeft aangevoerd dat het in de Verenigde Staten geldende recht en de daar gangbare praktijk geen waarborgen bieden voor voldoende bescherming tegen de toegang door de overheid tot de naar dit land doorgegeven gegevens. Deze klacht werd afgewezen op grond dat de Commissie in beschikking 2000/520 [79] had vastgesteld dat de Verenigde Staten een passend beschermingsniveau waarborgden. Bij arrest van 6 oktober 2015 heeft het Hof naar aanleiding van een prejudiciële vraag van de High Court (rechter in eerste aanleg, Ierland) deze beschikking ongeldig verklaard (hierna: „Schrems I-arrest")[80].

Na het Schrems I-arrest en de daaropvolgende nietigverklaring door de Ierse rechter van de beslissing waarbij de klacht van Schrems werd afgewezen, heeft de Ierse toezichthoudende autoriteit Schrems uitgenodigd om zijn klacht te herformuleren,

---

76 Artikel 45 AVG.

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

78 Artikel 49 AVG.

79 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).

80 Arrest van het Hof van 6 oktober 2015, Schrems, C-362/14, *EU:C:2015:650*.

gezien de ongeldigverklaring door het Hof van beschikking 2000/520. In zijn geherformuleerde klacht blijft Schrems erbij dat de Verenigde Staten geen passende bescherming bieden met betrekking tot naar dat land doorgegeven gegevens. Hij verzoekt de doorgifte van zijn persoonsgegevens vanuit de Unie naar de Verenigde Staten – die Facebook Ireland ondertussen uitvoert op grond van de standaardbepalingen inzake gegevensbescherming uit de bijlage bij besluit 2010/87/EU [81] – op te schorten of voor de toekomst te verbieden. 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. Na de inleiding van deze procedure heeft de Commissie uitvoeringsbesluit (EU) 2016/1250 betreffende de gepastheid van de door het EU-VS-privacyschild geboden bescherming[82] vastgesteld.

Met zijn verzoek om een prejudiciële beslissing stelt de verwijzende rechter het Hof vragen over de toepasselijkheid van de AVG op de doorgifte van persoonsgegevens op basis van de bij besluit 2010/87 vastgestelde standaardbepalingen inzake gegevensbescherming, het door de AVG vereiste beschermingsniveau bij een dergelijke doorgifte, en de verplichtingen die in dit verband rusten op toezichthoudende autoriteiten. 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. Besluit 2016/1250 wordt daarentegen ongeldig verklaard.

Het Hof is eerst en vooral van oordeel dat het Unierecht, en met name de AVG, van toepassing is op een doorgifte van persoonsgegevens voor commerciële doeleinden door een in een lidstaat gevestigde onderneming naar een andere in een derde land gevestigde onderneming, ook al kunnen deze gegevens tijdens of na die doorgifte door de autoriteiten van het derde land worden verwerkt ten behoeve van de openbare veiligheid, defensie en staatsveiligheid. Het Hof wijst erop dat een dergelijke verwerking van persoonsgegevens door de autoriteiten van een derde land niet kan worden uitgesloten van de werkingssfeer van de AVG.

Wat het vereiste beschermingsniveau bij een dergelijke doorgifte betreft, oordeelt het Hof dat de eisen in de AVG met betrekking tot passende waarborgen, afdwingbare rechten en doeltreffende rechtsmiddelen aldus moeten worden uitgelegd dat aan personen van wie persoonsgegevens naar een derde land worden doorgegeven op basis van standaardbepalingen inzake gegevensbescherming, een beschermingsniveau moet worden geboden dat in grote lijnen overeenkomt met het beschermingsniveau dat binnen de Unie wordt gewaarborgd door die verordening, gelezen in het licht van het

---

[81] 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).

[82] 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).

Handvest. Het Hof geeft aan dat bij de beoordeling van dit beschermingsniveau rekening moet worden gehouden met zowel 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 de eventuele toegang van de overheidsinstanties van dat derde land tot de doorgegeven gegevens betreft, de relevante aspecten van het rechtsstelsel van dat land.

Met betrekking tot de verplichtingen die de toezichthoudende autoriteiten bij de doorgifte hebben, oordeelt het Hof dat, tenzij de Commissie op geldige wijze een adequaatheidsbesluit heeft vastgesteld, deze autoriteiten verplicht zijn om een doorgifte van gegevens 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 door het Unierecht vereiste bescherming van de doorgegeven gegevens niet kan worden gewaarborgd met andere middelen, indien de in de Unie gevestigde exporteur de doorgifte niet zelf heeft opgeschort of beëindigd.

Het Hof heeft vervolgens de geldigheid van besluit 2010/87 onderzocht. Volgens het Hof kan het enkele feit dat de daarin opgenomen standaardbepalingen inzake gegevensbescherming door hun contractuele aard niet bindend zijn voor de autoriteiten van het derde land waarnaar persoonsgegevens kunnen worden doorgegeven, niet afdoen aan de geldigheid van dit besluit. Voor de geldigheid is daarentegen bepalend of dat besluit doeltreffende mechanismen bevat waarmee in de praktijk kan worden gewaarborgd dat het door het Unierecht vereiste beschermingsniveau in acht wordt genomen 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. Het benadrukt dat dit besluit een verplichting invoert voor de gegevensexporteur en de ontvanger van de doorgifte om vooraf na te gaan of het beschermingsniveau in acht wordt genomen in het derde land, en dat het besluit de ontvanger verplicht om de gegevensexporteur in kennis te stellen indien hij niet in staat zou zijn om de standaardbepalingen inzake gegevensbescherming na te leven. De gegevensexporteur moet in dat geval de doorgifte van gegevens opschorten en/of de overeenkomst met de ontvanger beëindigen.

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 constateringen in dit besluit merkt het Hof op dat voor sommige surveillanceprogramma's op geen enkele wijze uit die regeling blijkt dat er beperkingen gelden voor de daarin vervatte bevoegdheid tot uitvoering van die programma's of dat er garanties bestaan voor niet-Amerikanen die potentieel in het oog worden gehouden. Het Hof voegt hieraan toe dat die regeling weliswaar eisen stelt die door de Amerikaanse autoriteiten moeten worden nageleefd bij de uitvoering van surveillanceprogramma's, maar dat aan de betrokkenen geen voor de rechter afdwingbare rechten tegenover de Amerikaanse autoriteiten worden toegekend.

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 verklaart het Hof besluit 2016/1250 ongeldig.

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 de rubrieken II.1 „Werkingssfeer van de algemene regeling" en 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.

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. Indien dus na een verzoek van de betrokkene wordt vastgesteld dat de opneming van deze koppelingen in de lijst thans onverenigbaar is met de richtlijn, moeten deze informatie en koppelingen van die lijst worden gewist. 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.

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 informatie in kwestie 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.

2. Verwerking van persoonsgegevens en intellectuele-eigendomsrechten

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

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.

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")[83], 2001/29/EG betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij[84], 2004/48/EG betreffende de handhaving van intellectuele-eigendomsrechten[85], 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.

---

83 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).

84 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).

85 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).

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 tussen Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB en Storyside AB (hierna: „Bonnier Audio e.a.") en 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.

In dit verband heeft het Hof opgemerkt dat ingevolge de nationale wettelijke regeling in kwestie 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.

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.

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)

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 gevolg te geven aan de verzoeken van vier personen om verschillende links naar door derden gepubliceerde webpagina's, meer bepaald persartikelen, te verwijderen uit de resultatenlijst die na een zoekopdracht op hun respectieve namen door de zoekmachine werd weergegeven. Naar aanleiding van de klachten van deze vier personen heeft de Commission nationale de l'informatique et des libertés (nationale commissie voor informatica en vrijheden, CNIL) (Frankrijk) geweigerd Google aan te manen om de gevraagde verwijdering door te voeren. De Conseil d'État (hoogste bestuursrechter, Frankrijk), waarbij de zaak aanhangig is gemaakt, heeft het Hof verzocht om verduidelijking van de verplichtingen van de exploitant van een zoekmachine bij de behandeling van een verzoek tot verwijdering van links uit zoekresultaten krachtens richtlijn 95/46.

Ten eerste heeft het Hof eraan herinnerd dat de verwerking van persoonsgegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, het lidmaatschap van een vakvereniging, alsmede de verwerking van gegevens die de gezondheid en het seksuele leven betreffen verboden is[86], behoudens enkele uitzonderingen en afwijkingen. Gegevens inzake strafbare feiten, strafrechtelijke veroordelingen of veiligheidsmaatregelen mogen in beginsel alleen worden verwerkt onder toezicht van de overheid of indien het nationale recht passende en specifieke waarborgen biedt.[87]

Het Hof heeft geoordeeld dat het verbod en de beperkingen met betrekking tot de verwerking van deze bijzondere categorieën gegevens van toepassing zijn op de exploitant van een zoekmachine, net als op elke andere voor de verwerking van

---

86 Artikel 8, lid 1, van richtlijn 95/46 en artikel 9, lid 1, van verordening 2016/679.
87 Artikel 8, lid 5, van richtlijn 95/46 en artikel 10 van verordening 2016/679.

persoonsgegevens verantwoordelijke. Deze verboden en beperkingen hebben namelijk tot doel een betere bescherming te waarborgen tegen een dergelijke verwerking, die vanwege de bijzondere gevoeligheid van de gegevens in zeer ernstige mate inbreuk kan maken op de grondrechten op de eerbiediging van het privéleven en de bescherming van persoonsgegevens.

De exploitant van een zoekmachine is echter niet verantwoordelijk voor het feit dat persoonsgegevens op een door een derde gepubliceerde webpagina staan, maar voor de indexering van die pagina. In deze omstandigheden gelden het verbod en de beperkingen met betrekking tot de verwerking van gevoelige gegevens alleen voor deze exploitant op grond van het feit dat hij deze indexering verricht, waarbij dus onder toezicht van de bevoegde nationale autoriteiten en op basis van een door de betrokkene ingediend verzoek dient te worden getoetst of de exploitant zich daaraan houdt.

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[88], 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[89].

In ieder geval moet de exploitant van een zoekmachine bij de ontvangst van een verzoek tot verwijdering van links nagaan of de opname van de link naar een webpagina waarop gevoelige gegevens zijn gepubliceerd in de resultatenlijst die wordt weergegeven na een zoekopdracht op de naam van deze persoon strikt noodzakelijk is ter bescherming van de vrijheid van informatie van de internetgebruikers die mogelijk geïnteresseerd zijn in toegang tot die webpagina via een dergelijke zoekopdracht. In dit verband herinnert het Hof eraan dat, ofschoon de rechten op de eerbiediging van het privéleven en op de bescherming van persoonsgegevens in de regel prevaleren boven de vrijheid van informatie van de internetgebruikers, dit evenwicht in bijzondere gevallen kan afhangen van de aard van de betrokken informatie en de gevoeligheid ervan voor het privéleven van de betrokkene, alsook van het belang van het publiek, dat met name kan variëren naargelang van de rol die deze persoon in het openbare leven speelt.

Ten derde heeft het Hof geoordeeld dat het, in het kader van een verzoek om links naar gegevens inzake een strafrechtelijke procedure tegen de betrokkene die betrekking hebben op een voorgaande fase van die procedure en niet langer overeenkomen met de huidige situatie, uit zoekresultaten te verwijderen, aan de exploitant van een zoekmachine is om te toetsen of deze persoon, gelet op alle omstandigheden van het geval, 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

---

88 Artikel 8, lid 2, onder e), van richtlijn 95/46 en artikel 9, lid 2, onder e), van verordening 2016/679.

89 Artikel 14, eerste alinea, onder a), van richtlijn 95/46 en artikel 21, lid 1, van verordening 2016/679.

een op deze naam verrichte zoekopdracht. Zelfs indien dat niet het geval is omdat de opname van de betreffende link strikt noodzakelijk blijkt om de rechten van de betrokkene op eerbiediging van zijn privéleven en op bescherming van zijn gegevens te rijmen met de vrijheid van informatie van mogelijk geïnteresseerde internetgebruikers, dient de exploitant echter, uiterlijk bij het verzoek tot verwijdering van links uit zoekresultaten, de resultatenlijst dusdanig 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.

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

De Commission nationale de l'informatique et des libertés (CNIL) (nationale commissie voor informatica en vrijheden, Frankrijk) heeft Google aangemaand om bij het inwilligen van een verzoek tot verwijdering van links naar webpagina's waarop persoonsgegevens van een persoon voorkomen, deze links voor alle domeinnaamextensies van haar zoekmachine te verwijderen uit de resultatenlijst die wordt weergegeven na een zoekopdracht op de naam van de betrokkene. 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 (hoogste bestuursrechter, Frankrijk), waarbij Google de zaak aanhangig had gemaakt, heeft het Hof verzocht om de territoriale werkingssfeer van de verplichting voor de exploitant van een zoekmachine om uitvoering te geven aan het recht op verwijdering van links op grond van richtlijn 95/46 nader te bepalen.

Om te beginnen heeft het Hof in herinnering gebracht dat natuurlijke personen op grond van het Unierecht hun recht op verwijdering van links kunnen uitoefenen 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 de persoonsgegevens (in casu de indexering van links naar webpagina's met daarop de persoonsgegevens van de persoon die zich op dat recht beroept) in de Unie plaatsvindt.[90]

Wat betreft de werkingssfeer van het recht op verwijdering van links heeft het Hof geoordeeld dat de exploitant van een zoekmachine niet gehouden is deze links te verwijderen voor alle versies van zijn zoekmachine, maar enkel voor alle lidstaatspecifieke versies ervan. In dit verband heeft het Hof opgemerkt dat een universele verwijdering van links, gelet op de kenmerken van het internet en van zoekmachines, weliswaar ten volle kan beantwoorden aan de doelstelling van de Uniewetgever die erin bestaat in de gehele Unie een hoog niveau van bescherming van persoonsgegevens te waarborgen, maar dat geenszins uit het Unierecht[91] blijkt dat de wetgever ter verwezenlijking van deze doelstelling ervoor heeft gekozen om aan het recht op verwijdering van links een werkingssfeer toe te kennen die verder reikt dan het

---

90 Artikel 4, lid 1, onder a), van richtlijn 95/46, en artikel 3, lid 1, van verordening 2016/679.

91 Artikel 12, onder b), en 14, eerste alinea, onder a), van richtlijn 95/46, en artikel 17, lid 1, van verordening 2016/679.

grondgebied van de lidstaten. Het Unierecht heeft weliswaar mechanismen van samenwerking tussen de toezichthoudende autoriteiten van de lidstaten tot stand gebracht om te komen tot een gezamenlijk besluit dat gebaseerd is op een afweging tussen het recht op bescherming van het privéleven en van de persoonsgegevens enerzijds en het belang van het publiek van de verschillende lidstaten om toegang te hebben tot bepaalde informatie anderzijds, maar het voorziet thans met name niet in dergelijke mechanismen voor samenwerking wat betreft de reikwijdte van de verwijdering van links buiten de Unie.

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

Ten slotte benadrukt het Hof dat het Unierecht de exploitant van een zoekmachine weliswaar niet verplicht om links voor alle versies van zijn zoekmachine te verwijderen, maar dat 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 betrokken persoon 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 links te verwijderen voor alle versies van die zoekmachine.

Arrest van 8 december 2022 (Grote kamer), Google (Verwijdering van vermeend onjuiste inhoud) (C-460/20, EU:C:2022:962)

TU, die bij verschillende vennootschappen verantwoordelijke functies bekleedt en deelnemingen daarin heeft, en RE, diens partner en tot mei 2015 procuratiehouder van een van deze vennootschappen, zijn verzoekers in het hoofdgeding. Over hen heeft G LLC in 2015 op een website waarvan zijzelf de exploitant was, drie artikelen gepubliceerd. Daarvan was er één geïllustreerd met vier foto's van verzoekers die de suggestie wekten dat zij een luxueus leven leidden. In deze artikelen werd het investeringsmodel van meerdere van hun vennootschappen kritisch voorgesteld. De artikelen waren toegankelijk door in de zoekmachine van Google LLC (hierna: „Google") zoekopdracht in te geven op de voor- en achternamen van verzoekers, zowel afzonderlijk als in combinatie met bepaalde bedrijfsnamen. In de resultatenlijst werd met een link naar deze artikelen verwezen en waren de foto's opgenomen in de vorm van miniaturen („thumbnails").

Verzoekers in het hoofdgeding hebben Google als verantwoordelijke voor de met haar zoekmachine uitgevoerde verwerking van persoonsgegevens verzocht om ten eerste de links naar de betrokken artikelen uit de lijst met zoekresultaten te verwijderen, met het argument dat deze onjuiste beweringen en lasterlijke meningen bevatten, en ten tweede de miniaturen uit deze resultatenlijst te verwijderen. Google heeft dit verzoek afgewezen.

Nadat het beroep van verzoekers in het hoofdgeding zowel in eerste aanleg als in hoger beroep was afgewezen, hebben zij beroep in Revision ingesteld bij het Bundesgerichtshof (hoogste federale rechter in burgerlijke en strafzaken, Duitsland). In dat kader heeft het Bundesgerichtshof het Hof prejudiciële vragen over de uitlegging van de AVG en richtlijn 95/46 voorgelegd[92].

In zijn arrest, gewezen door de Grote kamer, werkt het Hof zijn rechtspraak over de voorwaarden waaronder de exploitant van een zoekmachine op grond van de regels inzake de bescherming van persoonsgegevens kan worden verzocht om links te verwijderen, verder uit. In het bijzonder onderzoekt het Hof ten eerste de omvang van de verplichtingen en verantwoordelijkheden van de exploitant van een zoekmachine bij de behandeling van een verzoek om links te verwijderen dat is gebaseerd op de vermeende onjuistheid van de informatie in de gelinkte inhoud, en ten tweede de bewijslast van de betrokkene met betrekking tot deze onjuistheid. Het Hof spreekt zich bovendien uit over de vraag of bij de toetsing van een verzoek om foto's te verwijderen die in de resultatenlijst van een zoekopdracht naar afbeeldingen zijn weergegeven in de vorm van miniaturen, noodzakelijkerwijs rekening moet worden gehouden met de context waarin deze foto's oorspronkelijk op internet zijn gepubliceerd.

In de eerste plaats verklaart het Hof voor recht dat in het kader van de afweging van de rechten op eerbiediging van het privéleven en op bescherming van persoonsgegevens enerzijds en het recht op vrijheid van meningsuiting en van informatie[93] anderzijds bij de toetsing van een tot de exploitant van een zoekmachine gericht verwijderingsverzoek dat ertoe strekt om een link naar inhoud die vermeend onjuiste informatie bevat te schrappen uit de lijst met zoekresultaten, niet als voorwaarde voor deze verwijdering geldt dat de vraag naar de juistheid van de gelinkte inhoud ten minste voorlopig is beslecht in het kader van een beroep van de verzoeker tegen de aanbieder van deze inhoud.

Wat de voorwaarden betreft waaronder de exploitant van een zoekmachine een verzoek tot verwijdering van links moet inwilligen en dus uit de na een zoekopdracht op de naam van de betrokken persoon weergegeven resultatenlijst de link moet schrappen die leidt naar een website met daarop beweringen die volgens deze persoon onjuist zijn, brengt het Hof vooraf met name het volgende in herinnering:

• aangezien de werking van een zoekmachine, bovenop de werkzaamheden van webredacteuren, de grondrechten op eerbiediging van het privéleven en op

---

92 Respectievelijk artikel 17, lid 3, onder a), AVG en artikel 12, onder b), en artikel 14, eerste alinea, onder a), van richtlijn 95/46.

93 Grondrechten die zijn gewaarborgd in respectievelijk de artikelen 7, 8 en 11 van het Handvest.

bescherming van persoonsgegevens aanzienlijk kan aantasten, moet de exploitant van deze zoekmachine – als persoon die het doel van en de middelen voor deze werking vaststelt – in het kader van zijn verantwoordelijkheden, zijn bevoegdheden en zijn mogelijkheden verzekeren dat de waarborgen van richtlijn 95/46 en de AVG hun volle werking kunnen krijgen en een doelmatige en volledige bescherming van de betrokkenen daadwerkelijk tot stand kan worden gebracht;

• wanneer bij de exploitant van een zoekmachine een verzoek tot verwijdering van links is ingediend, moet hij nagaan of de opname van de link naar de betrokken website op de resultatenlijst noodzakelijk is voor de uitoefening van het recht op vrijheid van informatie van internetgebruikers die deze website mogelijk zouden willen raadplegen door middel van een dergelijke door het recht op vrijheid van meningsuiting en van informatie beschermde zoekopdracht;

• de AVG vereist uitdrukkelijk dat er een afweging wordt gemaakt tussen de grondrechten op eerbiediging van het privéleven en op bescherming van persoonsgegevens enerzijds, en het grondrecht op vrijheid van informatie anderzijds.

Om te beginnen merkt het Hof op dat de rechten op eerbiediging van het privéleven en op bescherming van persoonsgegevens weliswaar in de regel voorrang hebben op het gerechtvaardigd belang van internetgebruikers om de betrokken informatie te raadplegen, maar dat dit evenwicht kan afhangen van de relevante omstandigheden van het geval, waaronder de aard van deze informatie en de gevoeligheid ervan voor het privéleven van de betrokkene en het belang dat het publiek erbij heeft om over deze informatie te beschikken. Dit belang kan met name variëren naargelang van de rol van deze persoon in het openbare leven.

De vraag of de inhoud waarnaar een link is opgenomen al dan niet juist is, is eveneens een relevant aspect bij deze beoordeling. In bepaalde omstandigheden kunnen het recht op informatie van internetgebruikers en de vrijheid van meningsuiting van de aanbieder van inhoud zwaarder wegen dan het recht op bescherming van het privéleven en het recht op bescherming van persoonsgegevens, met name wanneer de betrokkene een rol speelt in het openbare leven. De omgekeerde verhouding doet zich evenwel voor wanneer ten minste een – ten opzichte van de gehele inhoud – niet onbeduidend deel van de informatie waarop het verzoek tot verwijdering van links betrekking heeft, onjuist blijkt te zijn. In een dergelijk geval kan geen rekening worden gehouden met het recht op informatie en het recht om geïnformeerd te worden, aangezien het recht om dergelijke informatie te verspreiden en er toegang toe te krijgen, daar niet onder valt.

Wat vervolgens ten eerste de verplichtingen betreft die gelden bij de vaststelling of de informatie in de gelinkte inhoud al dan niet juist is, verduidelijkt het Hof dat de persoon die om verwijdering van links verzoekt met het argument dat dergelijke informatie onjuist is, moet aantonen dat die informatie, of ten minste een ten opzichte van die gehele inhoud niet onbeduidend deel daarvan, kennelijk onjuist is. Om te vermijden dat deze persoon een buitensporige last krijgt opgelegd die het nuttig effect van het recht op verwijdering van links kan ondermijnen, hoeft hij echter alleen bewijzen te leveren die, gelet op de omstandigheden van het geval, redelijkerwijs van hem kunnen worden verlangd. In beginsel is deze persoon niet verplicht om, ter ondersteuning van zijn verzoek om links te verwijderen, reeds in de precontentieuze fase een tegen de

webredacteur verkregen rechterlijke beslissing, zij het zelfs maar een beslissing in kort geding, over te leggen.

Wat ten tweede de verplichtingen en verantwoordelijkheden van de exploitant van de zoekmachine betreft, benadrukt het Hof dat deze exploitant zich bij de beoordeling of bepaalde inhoud verder mag worden opgenomen in de lijst met resultaten van zoekopdrachten die na een verzoek tot verwijdering van links via zijn zoekmachine worden verricht, moet baseren op alle betrokken rechten en belangen en op alle omstandigheden van het concrete geval. Deze exploitant is evenwel niet verplicht om de feiten te onderzoeken en daartoe een discussie aan te gaan met de aanbieder van inhoud om ontbrekende gegevens te verkrijgen over de juistheid van de gelinkte inhoud. Indien de exploitant zou worden verplicht om bij te dragen tot de vaststelling of de gelinkte inhoud al dan niet juist is, zou hem een last worden opgelegd die verder gaat dan wat redelijkerwijs van hem kan worden verwacht in het licht van zijn verantwoordelijkheden, bevoegdheden en mogelijkheden. Deze oplossing zou een ernstig risico met zich meebrengen dat links worden verwijderd die leiden naar inhoud die in een gerechtvaardigde en dwingende informatiebehoefte van het publiek voorziet, en het dus moeilijk wordt om deze inhoud op internet te vinden. Aldus zou er een reëel risico bestaan dat de uitoefening van de vrijheid van meningsuiting en van informatie ontmoedigd wordt indien een exploitant van een zoekmachine nagenoeg systematisch links zou verwijderen om te vermijden dat hij belast wordt met het onderzoek naar de feiten die relevant zijn om vast te stellen of de gelinkte inhoud al dan niet juist is.

Wanneer de persoon die heeft verzocht om verwijdering van links met bewijzen aantoont dat de informatie in de gelinkte inhoud, of ten minste een ten opzichte van die gehele gelinkte inhoud niet onbeduidend deel van die informatie, kennelijk onjuist is, moet de exploitant van de zoekmachine dit verzoek dus inwilligen. Hetzelfde geldt wanneer deze verzoeker een tegen de webredacteur gerichte rechterlijke beslissing overlegt die is gebaseerd op de vaststelling dat een ten opzichte van de gehele gelinkte inhoud niet onbeduidend deel daarvan op zijn minst op het eerste gezicht onjuist is. Indien daarentegen de onjuistheid van dergelijke informatie niet duidelijk blijkt uit het door de verzoeker overgelegde bewijsmateriaal, hoeft de exploitant van de zoekmachine het verzoek tot verwijdering van links niet in te willigen als een dergelijke rechterlijke beslissing ontbreekt. Wanneer de betrokken informatie bij kan dragen aan een debat van algemeen belang moet, gelet op alle omstandigheden van het concrete geval, bijzondere betekenis worden toegekend aan het recht op vrijheid van meningsuiting en van informatie.

Tot slot voegt het Hof daaraan toe dat de betrokkene, wanneer de exploitant van een zoekmachine een verzoek tot verwijdering van links niet inwilligt, de mogelijkheid moet hebben om zich te wenden tot de toezichthoudende autoriteit of tot de rechter, opdat die de nodige controles kan uitvoeren en de verantwoordelijke exploitant kan gelasten de nodige maatregelen te nemen. Met name de rechterlijke autoriteiten moeten de tegenstrijdige belangen afwegen, want zij zijn het best in staat een dergelijke complexe en grondige afweging te maken, waarbij rekening wordt gehouden met alle criteria en aspecten die in de relevante rechtspraak zijn vastgesteld.

In de tweede plaats verklaart het Hof voor recht dat in het kader van de afweging van bovengenoemde grondrechten met het oog op de toetsing van een verwijderingsverzoek dat ertoe strekt om in de vorm van miniaturen weergegeven foto's met daarop de afbeelding van een natuurlijke persoon te schrappen uit de resultaten van een zoekopdracht naar afbeeldingen op de naam van die persoon, rekening moet worden gehouden met de informatieve waarde van deze foto's, los van de oorspronkelijke context van de publicatie ervan op de website waarvan zij afkomstig zijn. Daarbij moet wel alle tekst in aanmerking worden genomen die vlak bij de weergave van deze foto's in de zoekresultaten is geplaatst en meer duidelijkheid kan geven over de informatieve waarde daarvan.

Ter ondersteuning van deze slotsom benadrukt het Hof dat voor zoekopdrachten naar afbeeldingen op de naam van een persoon die op internet met een zoekmachine worden verricht, dezelfde beginselen gelden als voor zoekopdrachten naar websites en de daarin vervatte informatie. Als na een zoekopdracht op naam foto's van de betrokkene in de vorm van miniaturen worden weergegeven, kan deze weergave volgens het Hof een bijzonder belangrijke inmenging vormen in de rechten op bescherming van het privéleven en de persoonsgegevens van deze persoon.

Wanneer bij de exploitant van een zoekmachine een verwijderingsverzoek is ingediend dat ertoe strekt om in de vorm van miniaturen weergegeven foto's met daarop de afbeelding van een persoon te schrappen uit de resultaten van een zoekopdracht naar afbeeldingen op de naam van die persoon, moet hij dus nagaan of de weergave van de betrokken foto's noodzakelijk is voor de uitoefening van het recht op vrijheid van informatie van internetgebruikers die mogelijk via een dergelijke zoekopdracht toegang zouden willen krijgen tot deze foto's.

Voor zover de zoekmachine foto's van de betrokkene toont buiten de context waarin zij op de gelinkte website zijn gepubliceerd, welke publicatie meestal tot doel heeft om de op deze site weergegeven tekst te illustreren, moet worden vastgesteld of deze context niettemin in aanmerking moet worden genomen bij de te verrichten afweging van botsende rechten en belangen. In dit verband is het antwoord op de vraag of die beoordeling ook moet slaan op de inhoud van de website met daarop de foto waarvan de miniatuurweergave volgens het verzoek verwijderd moet worden, afhankelijk van het voorwerp en de aard van de betrokken verwerking.

Wat ten eerste het voorwerp van de betrokken verwerking betreft, merkt het Hof op dat de publicatie van foto's als niet-verbaal communicatiemiddel van grotere invloed kan zijn op internetgebruikers dan gepubliceerde teksten. Foto's zijn als zodanig immers een belangrijk middel om de aandacht van internetgebruikers te trekken en kunnen bij hen de zin opwekken om de met deze foto's geïllustreerde artikelen te raadplegen. Met name omdat foto's vaak voor meerdere uitleg vatbaar zijn, kan de miniatuurweergave ervan in de resultatenlijst van de zoekopdracht leiden tot een bijzonder ernstige inmenging in het recht van de betrokkene op bescherming van zijn beeltenis. Dit moet in aanmerking worden genomen bij de afweging van botsende rechten en belangen. Er moeten verschillende afwegingen worden gemaakt naargelang het gaat om door de redacteur van de website gepubliceerde artikelen met foto's die in hun oorspronkelijke context zijn opgenomen en de in die artikelen verstrekte informatie en de daarin geuite

meningen illustreren, dan wel om foto's die de exploitant van een zoekmachine, los van de context waarin zij op de oorspronkelijke website zijn gepubliceerd, in de vorm van miniaturen weergeeft in de lijst met zoekresultaten.

In dit verband merkt het Hof niet alleen op dat de grond die de publicatie van persoonsgegevens op een website rechtvaardigt, niet noodzakelijkerwijze dezelfde is als die welke de werkwijze van zoekmachines rechtvaardigt, maar ook dat zelfs wanneer dit het geval is, de te maken afweging tussen de betrokken belangen tot een verschillend resultaat kan leiden naargelang het gaat om een verwerking door de exploitant van een zoekmachine dan wel om een verwerking door de redacteur van deze website. Ten eerste kunnen de rechtmatige belangen die deze verwerkingen rechtvaardigen verschillend zijn, en ten tweede zijn de gevolgen van deze verwerkingen voor de betrokkene, en met name voor zijn privéleven, niet noodzakelijkerwijze dezelfde.

Wat ten tweede de aard van de door de exploitant van de zoekmachine verrichte verwerking betreft, stelt het Hof vast dat de exploitant van een zoekmachine, door op internet gepubliceerde foto's van natuurlijke personen te verzamelen en deze afzonderlijk in de vorm van miniaturen in de resultaten van een zoekopdracht naar afbeeldingen weer te geven, een dienst aanbiedt waarbij een autonome verwerking van persoonsgegevens plaatsvindt die zowel verschilt van de verwerking door de redacteur van de website waarvan de foto's afkomstig zijn als van de verwerking die wordt verricht bij de opname van een link naar deze site, waarvoor deze exploitant eveneens verantwoordelijk is.

Bijgevolg moeten de werkzaamheden van de exploitant van de zoekmachine, die erin bestaan de resultaten van een zoekopdracht naar afbeeldingen in de vorm van miniaturen weer te geven, autonoom worden beoordeeld. De aanvullende inbreuk op de grondrechten die hieruit voortvloeit kan namelijk bijzonder ernstig zijn, omdat bij een zoekopdracht op naam alle op internet te vinden informatie over de betrokken persoon wordt samengevoegd. Bij deze autonome beoordeling moet er rekening mee worden gehouden dat deze weergave op zich het door de internetgebruiker nagestreefde resultaat vormt, los van zijn latere beslissing om de oorspronkelijke internetpagina al dan niet te raadplegen.

Het Hof merkt evenwel op dat een dergelijke specifieke afweging, waarbij de autonome aard van de door de exploitant van de zoekmachine verrichte verwerking in aanmerking wordt genomen, niet afdoet aan de eventuele relevantie van tekst die vlak bij de weergave van een foto in de resultatenlijst van een zoekopdracht kan zijn geplaatst, aangezien die meer duidelijkheid kan geven over de informatieve waarde van deze foto voor het publiek en dus van invloed kan zijn op de afweging van de betrokken rechten en belangen.

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

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

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. Bovendien heeft het Hof verduidelijkt dat de aanbieder van diensten de gebruiker van een website erop moet wijzen hoelang de cookies actief blijven en of derden al dan niet toegang tot de cookies kunnen hebben.

Het hoofdgeding had betrekking op een reclameloterij die Planet49 had georganiseerd op de website www.dein-macbook.de. Om te kunnen deelnemen moesten internetgebruikers hun naam en adres opgeven op een website met selectievakjes. Het vakje waarmee toestemming werd gegeven voor de installatie van cookies was standaard aangevinkt. Het Bundesgerichtshof (hoogste federale rechter in burgerlijke en strafzaken, Duitsland), waarbij de Duitse federale vereniging van consumentenbeschermingsorganisaties beroep had ingesteld, had twijfels over de geldigheid van toestemming die gebruikers hebben verleend door middel van het standaard aangevinkte selectievakje en over de omvang van de informatieverplichting waaraan de aanbieder van diensten moet voldoen.

Het verzoek om een prejudiciële beslissing had hoofdzakelijk betrekking op de uitlegging van het begrip „toestemming” als bedoeld in richtlijn 2002/58 [94], gelezen in samenhang met richtlijn 95/46/EG[95] en met de AVG[96].

Het Hof heeft ten eerste opgemerkt dat artikel 2, onder h) van richtlijn 95/46/EG, waarnaar in artikel 2, onder f), van richtlijn 2002/58 wordt verwezen, de 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 aangegeven dat met de eis van een „wilsuiting” van de betrokkene duidelijk wordt verwezen naar een actieve en niet naar een passieve gedraging. Toestemming door middel van een standaard aangevinkt selectievakje impliceert echter geen actieve gedraging van de gebruiker van een website. 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 – lijkt er bovendien op 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 tegenwoordig voorzien in actieve toestemming in de AVG[97], die

---

[94] 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 woensdag 25 november 2009 (PB 2009, L 337, blz. 11).

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

[96] Artikel 6, lid 1, onder a), van verordening 2016/679

[97] Idem.

in artikel 4, punt 11, een wilsuiting vereist in de vorm van met name een „ondubbelzinnige actieve handeling” en in overweging 32 uitdrukkelijk uitsluit dat er sprake is van toestemming in geval van „stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit”.

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 op 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 toestemming te verlenen. Het heeft daaraan toegevoegd dat het feit dat de gebruiker op de knop voor deelname aan de betrokken reclameloterij heeft geklikt, op zich niet kan volstaan om vast te stellen dat hij rechtsgeldig toestemming heeft verleend voor het plaatsen van cookies.

Ten tweede heeft het Hof vastgesteld dat met artikel 5, lid 3, van richtlijn 2002/58 is beoogd de gebruiker te beschermen tegen elke inmenging in zijn privéleven, ongeacht of die inmenging betrekking heeft op persoonsgegevens. Hieruit vloeit voort dat het begrip „toestemming” niet anders moet worden uitgelegd naargelang de informatie die is opgeslagen op de eindapparatuur van de gebruiker van een website of daaruit is opgevraagd, al dan niet bestaat in persoonsgegevens.

Ten derde heeft het Hof opgemerkt dat artikel 5, lid 3, van richtlijn 2002/58 vereist dat de gebruiker zijn toestemming heeft verleend na te zijn voorzien van duidelijke en volledige informatie over onder meer het doel 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 vastgesteld dat de informatie hoelang de cookies actief blijven en of derden al dan niet toegang tot de cookies kunnen hebben, deel uitmaakt van de duidelijke en volledige informatie die de aanbieder van diensten aan de gebruiker van een website moet verstrekken.

5. Verwerking van persoonsgegevens op online sociale netwerken

Arrest van 4 juli 2023 (Grote kamer), Meta Platforms e.a. (Algemene gebruiksvoorwaarden van een sociaal netwerk) (C-252/21, EU:C:2023:537)

Meta Platforms is eigenaar van het online sociale netwerk Facebook, dat voor particuliere gebruikers gratis is. Het bedrijfsmodel van dit online sociale netwerk is erop gebaseerd inkomsten te verwerven met onlinereclame die specifiek op de individuele gebruikers is toegesneden. Technisch gezien is die gepersonaliseerde reclame mogelijk doordat automatisch gedetailleerde profielen worden opgesteld van de gebruikers van dit netwerk en van de overige onlinediensten die door het Metaconcern worden aangeboden. Daarom kan dit sociale netwerk alleen worden gebruikt door degene die bij de registratie akkoord gaat met de algemene voorwaarden van Meta Platforms, die verwijzen naar haar gegevens- en cookiebeleid. Op grond van dat beleid verzamelt Meta

Platforms naast de gegevens die de gebruikers rechtstreeks bij hun inschrijving verstrekken ook gegevens over hun activiteiten binnen en buiten het sociale netwerk en koppelt zij deze gegevens aan de Facebookaccounts van de betrokken gebruikers. De gegevens over activiteiten buiten het sociale netwerk – die ook worden aangeduid als „off-Facebook-gegevens” – betreffen bezoeken aan websites en apps van derden alsook het gebruik van andere onlinediensten van het Metaconcern (waaronder Instagram en WhatsApp). Uit alle aldus verzamelde gegevens bij elkaar kunnen gedetailleerde conclusies worden getrokken over voorkeuren en interesses van deze gebruikers.

Bij besluit van 6 februari 2019 heeft het Bundeskartellamt (federale mededingingsautoriteit, Duitsland) Meta Platforms verboden om in de toen geldende algemene voorwaarden het gebruik van het online sociale netwerk Facebook door in Duitsland wonende particuliere gebruikers afhankelijk te stellen van de verwerking van hun off-Facebook-gegevens, en om deze gegevens zonder hun toestemming te verwerken. Verder heeft het Bundeskartellamt haar gelast om haar algemene voorwaarden zodanig aan te passen dat daaruit duidelijk blijkt dat die gegevens niet zonder toestemming van de betreffende gebruikers verzameld, met de Facebook-gebruikersaccounts gekoppeld en gebruikt zullen worden. Ten slotte heeft deze autoriteit benadrukt dat een dergelijke toestemming ongeldig is wanneer zij een voorwaarde vormt om het online sociale netwerk te kunnen gebruiken. Het Bundeskartellamt heeft ter motivering van zijn besluit uiteengezet dat Meta Platforms met de betrokken gegevensverwerking, die niet in overeenstemming is met de AVG, misbruik maakt van haar machtspositie op de markt van online sociale netwerken.

Meta Platforms heeft tegen dat besluit beroep ingesteld bij het Oberlandesgericht Düsseldorf (hoogste rechterlijke instantie van de deelstaat Noordrijn-Westfalen, Düsseldorf, Duitsland). Aangezien deze rechter twijfels had over de uitlegging van verschillende bepalingen van de AVG, heeft hij het Hof om een prejudiciële beslissing verzocht.

In zijn arrest geeft het Hof (Grote kamer) verduidelijkingen over de mogelijkheden van een exploitant van een online sociaal netwerk om „gevoelige” persoonsgegevens van de gebruikers van dit netwerk te verwerken, over de voorwaarden waaronder de gegevensverwerking door een dergelijke exploitant op rechtmatige wijze plaatsvindt en over de geldigheid van de toestemming voor een dergelijke verwerking die deze gebruikers verlenen aan een onderneming met een machtspositie op de nationale markt van online sociale netwerken.

Wat de verwerking van bijzondere categorieën persoonsgegevens[98] betreft, is het Hof van oordeel dat wanneer een gebruiker van een online sociaal netwerk websites of apps bezoekt die met een of meer van die categorieën verband houden, en in voorkomend geval daar gegevens invoert door zich te registreren of online bestellingen te plaatsen,

---

[98] Zoals vastgelegd in artikel 9, lid 1, AVG. Volgens deze bepaling zijn de „[v]erwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en [de] verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid [...] verboden”.

de verwerking van persoonsgegevens door de exploitant van dat online sociale netwerk[99] moet worden beschouwd als een „verwerking van bijzondere categorieën persoonsgegevens" in de zin van artikel 9, lid 1, AVG, wanneer bij deze gegevensverwerking informatie aan het licht kan komen die onder een van deze bijzondere categorieën valt, ongeacht of deze informatie betrekking heeft op een gebruiker van dat netwerk of op een andere natuurlijke persoon. Een dergelijke verwerking van gegevens is in beginsel verboden, behoudens bepaalde uitzonderingen.[100]

In verband met dit laatste punt verduidelijkt het Hof dat een gebruiker van een online sociaal netwerk die websites of apps bezoekt die met een of meer van die bijzondere gegevenscategorieën verband houden, de gegevens over deze bezoeken die door de exploitant van dit online sociale netwerk via cookies of soortgelijke registratietechnologieën worden verzameld, niet kennelijk openbaar maakt[101]. Wanneer zo'n gebruiker op dergelijke websites of apps gegevens invoert of wanneer hij daarin geïntegreerde selectieknoppen aanklikt – zoals de knoppen „vind ik leuk" of „delen", of de knoppen waarmee hij zich op deze websites of apps kan identificeren met behulp van de inloggegevens die zijn gekoppeld aan zijn gebruikersaccount van het online sociale netwerk, zijn telefoonnummer of zijn e-mailadres –, maakt hij de aldus ingevoerde of uit het aanklikken van deze knoppen voortvloeiende gegevens slechts kennelijk openbaar wanneer hij vooraf uitdrukkelijk zijn keuze kenbaar heeft gemaakt, in voorkomend geval op basis van een met volledige kennis van zaken uitgevoerde individuele configuratie, om de hem betreffende gegevens openbaar te maken voor een onbeperkt aantal personen.

Wat meer in het algemeen de voorwaarden betreft waaronder een verwerking van persoonsgegevens rechtmatig is, wijst het Hof erop dat de verwerking van persoonsgegevens volgens de AVG alleen rechtmatig is indien en voor zover de betrokkene daar voor een of meer specifieke doeleinden toestemming voor heeft gegeven[102]. Bij gebreke van een dergelijke toestemming of wanneer die toestemming niet vrij, specifiek, geïnformeerd en ondubbelzinnig is gegeven, is een dergelijke verwerking niettemin gerechtvaardigd wanneer is voldaan aan een van de voorwaarden waarbij er sprake is van noodzakelijkheid[103], die strikt moeten worden uitgelegd. De

---

99 Deze verwerking bestaat erin dat deze exploitant, door middel van geïntegreerde interfaces, cookies of soortgelijke registratietechnologieën, de gegevens die voortvloeien uit bezoeken aan die websites en apps alsook de gegevens die door de gebruiker zijn ingevoerd verzamelt, al deze gegevens koppelt aan het account van deze laatste bij het online sociale netwerk en die gegevens gebruikt.

100 Zoals vastgelegd in artikel 9, lid 2, AVG. Die bepaling luidt als volgt: „Lid 1 is niet van toepassing wanneer aan een van de onderstaande voorwaarden is voldaan:

a) de betrokkene heeft uitdrukkelijke toestemming gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden, behalve indien in Unierecht of lidstatelijk recht is bepaald dat het in lid 1 genoemde verbod niet door de betrokkene kan worden opgeheven; […]

e) de verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;

f) de verwerking is noodzakelijk voor de instelling, uitoefening of verdediging van een rechtsvordering of wanneer gerechten handelen in het kader van hun rechtsprekende taken;

[…]".

101 In de zin van artikel 9, lid 2, onder e), AVG.

102 In de bewoordingen van artikel 6, lid 1, eerste alinea, onder a), AVG.

103 Vermeld in artikel 6, lid 1, eerste alinea, onder b) tot en met f), AVG. Volgens deze bepalingen is de verwerking alleen rechtmatig indien en voor zover zij noodzakelijk is voor onder meer de uitvoering van een overeenkomst waarbij de betrokkene partij is [artikel 6, lid 1, eerste alinea, onder b), AVG], om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust [artikel 6, lid 1, eerste

verwerking van persoonsgegevens van de gebruikers van een online sociaal netwerk die door de exploitant van dat netwerk wordt verricht kan slechts noodzakelijk worden geacht voor de uitvoering van de overeenkomst waarbij deze gebruikers partij zijn, indien die verwerking objectief onontbeerlijk is om een doel te bereiken dat een integrerend deel uitmaakt van de aan deze gebruikers te leveren contractuele prestatie, zodat het hoofddoel van de overeenkomst zonder die verwerking niet zou kunnen worden bereikt.

Verder kan de betrokken gegevensverwerking volgens het Hof slechts noodzakelijk worden geacht voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde indien die exploitant de gebruikers bij wie de gegevens zijn verzameld, heeft meegedeeld dat er met de verwerking een gerechtvaardigd belang wordt behartigd, indien deze verwerking binnen de grenzen blijft van hetgeen voor de behartiging van dat belang strikt noodzakelijk is en indien uit een afweging van de tegengestelde belangen in het licht van alle relevante omstandigheden blijkt dat de belangen of grondrechten en fundamentele vrijheden van die gebruikers niet zwaarder wegen dan dit gerechtvaardigde belang van de verwerkingsverantwoordelijke of van een derde. Het Hof is met name van oordeel dat de belangen en grondrechten van deze gebruikers, ingeval zij geen toestemming hebben verleend, zwaarder wegen dan het belang dat de exploitant van een online sociaal netwerk heeft bij de personalisatie van de reclame waarmee hij zijn activiteit financiert.

Ten slotte verduidelijkt het Hof dat de betrokken gegevensverwerking gerechtvaardigd is wanneer zij daadwerkelijk noodzakelijk is om een wettelijke verplichting na te komen die krachtens een bepaling van Unierecht of het recht van de betrokken lidstaat op de verwerkingsverantwoordelijke rust, wanneer deze rechtsgrondslag beantwoordt aan een doelstelling van algemeen belang en evenredig is aan het nagestreefde gerechtvaardigde doel, en wanneer die verwerking binnen de grenzen van het strikt noodzakelijke blijft.

Wat de geldigheid betreft van de toestemming van de betrokken gebruikers voor de verwerking van hun gegevens krachtens de AVG, is het Hof van oordeel dat de omstandigheid dat de exploitant van een online sociaal netwerk een machtspositie inneemt op de markt van online sociale netwerken als zodanig er niet aan in de weg staat dat de gebruikers van een dergelijk netwerk rechtsgeldig kunnen instemmen met de verwerking van hun persoonsgegevens door die exploitant. Aangezien een dergelijke machtspositie de keuzevrijheid van deze gebruikers kan aantasten en kan leiden tot een duidelijke wanverhouding tussen hen en de exploitant, vormt zij evenwel een belangrijk element om te bepalen of de toestemming daadwerkelijk rechtsgeldig en met name vrijelijk is gegeven, hetgeen door die exploitant moet worden bewezen[104].

alinea, onder c), AVG] of voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde [artikel 6, lid 1, eerste alinea, onder f), AVG].

104 Krachtens artikel 7, lid 1, AVG.

De gebruikers van het desbetreffende online sociale netwerk moeten in het bijzonder de vrijheid hebben om tijdens het sluiten van de overeenkomst hun toestemming voor bijzondere gegevensverwerkingshandelingen die niet noodzakelijk zijn voor de uitvoering van de overeenkomst, voor elke verwerking apart te weigeren zonder ertoe te worden gedwongen om volledig van het gebruik van het online sociale netwerk af te zien, hetgeen betekent dat zij, in voorkomend geval tegen een passende vergoeding, een gelijkwaardig alternatief moeten krijgen aangeboden dat niet met een dergelijke gegevensverwerking gepaard gaat. Ook voor de verwerking van de off-Facebook-gegevens moet afzonderlijke toestemming kunnen worden gegeven.

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***)***

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 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.

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, zij het 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. Bovendien vereist de door deze toezichthoudende autoriteiten vervulde rol van hoeders van het recht op bescherming van de persoonlijke levenssfeer dat de beslissingen van deze 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.

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.

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 functionele onafhankelijkheid geniet, in die zin dat haar leden bij de uitoefening van hun functie onafhankelijk zijn en door geen enkele instructie zijn

gebonden, volstaat in dit verband 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.

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.

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

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.

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.

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 het gehele mandaat boven deze autoriteit hangende dreiging van een dergelijke voortijdige beëindiging kunnen leiden tot een vorm van gehoorzaamheid 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.

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)

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 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.

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. Toch 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.

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.

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.

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.

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).

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.

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 doen stellen 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[105] 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[106] 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 neergelegde „éénloket-beginsel", alleen de Ierse commissaris voor gegevensbescherming bevoegd om, onder toezicht van de Ierse rechterlijke instanties, een stakingsvordering in te stellen.

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

---

[105] Bijvoorbeeld „Vind ik leuk" of „Delen".

[106] Zie artikel 56, lid 1, AVG: „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".

en in rechte op te treden met betrekking tot een grensoverschrijdende gegevensverwerking[107], ook indien zij niet de leidende autoriteit voor die verwerking is.

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 samenwerkingsprocedure en het coherentiemechanisme die in die verordening zijn vastgelegd[108].

Voor grensoverschrijdende verwerkingen voorziet de AVG namelijk in het „één-loketmechanisme”[109], 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 vrijwaren. In dit verband ligt krachtens de AVG de competentie om een besluit te nemen waarbij wordt vastgesteld dat een grensoverschrijdende verwerking in strijd is met de in deze verordening vervatte regels in beginsel bij de leidende toezichthoudende autoriteit[110], terwijl de competentie van de andere nationale toezichthoudende autoriteiten om – zelfs maar voorlopig – een dergelijk besluit te nemen de uitzondering vormt.[111] 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.

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

---

107 In de zin van artikel 4, punt 23, AVG.
108 Die zijn opgenomen in artikel 56 en 60 AVG.
109 Artikel 56, lid 1, AVG.
110 Artikel 60, lid 7, AVG.
111 Artikel 56, lid 2, en artikel 66 AVG voorzien in uitzonderingen op het beginsel van de beslissingsbevoegdheid van de leidende toezichthoudende autoriteit.

andere toezichthoudende autoriteiten[112], 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.

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[113] 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[114] vallen, hetgeen veronderstelt dat de verwerkingsverantwoordelijke of de verwerker die de grensoverschrijdende verwerking verricht over een vestiging op het grondgebied van de Unie beschikt.

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 zijn, 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.

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

---

[112] Die zijn neergelegd in de artikelen 55 en 56, gelezen in samenhang met artikel 60 AVG.

[113] Op grond van artikel 58, lid 5, AVG.

[114] Artikel 3, lid 1 van deze verordening bepaalt dat zij 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 al dan niet plaatsvindt”.

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 samenwerkingsprocedure en het coherentiemechanisme die in die verordening zijn vastgelegd, in acht neemt.

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.

Arrest van 16 januari 2024 (Grote kamer), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

In deze zaak (zie tevens rubriek II.1, „Werkingssfeer van de algemene regeling”) merkt het Hof op dat de bepalingen van de AVG met betrekking tot de competentie van de nationale toezichthoudende autoriteiten en het recht om een klacht in te dienen[115] geen nationale uitvoeringsmaatregelen vereisen en voldoende duidelijk, nauwkeurig en onvoorwaardelijk zijn om rechtstreekse werking te hebben. Hieruit volgt dat de AVG de lidstaten weliswaar een beoordelingsmarge laat met betrekking tot het aantal in te stellen toezichthoudende autoriteiten[116], maar dat deze verordening wel bepaalt welke reikwijdte hun bevoegdheden hebben opdat zij toezicht houden op de toepassing van de verordening. Wanneer een lidstaat ervoor kiest om één enkele nationale toezichthoudende autoriteit in te stellen, beschikt deze autoriteit dus noodzakelijkerwijs over alle door de verordening toegekende bevoegdheden. Een andersluidende uitlegging zou afbreuk doen aan de effectiviteit van die bepalingen en zou de effectiviteit kunnen aantasten van alle andere bepalingen van de AVG die relevant zouden kunnen zijn voor een klacht.

Wat de omstandigheid betreft dat nationale constitutionele bepalingen eraan in de weg staan dat een toezichthoudende autoriteit die onderdeel is van de uitvoerende macht, toezicht kan uitoefenen op de toepassing van de AVG door een orgaan van de wetgevende macht, geeft het Hof aan dat het juist met het oog op de constitutionele structuur van de lidstaten is dat de AVG slechts vereist dat de lidstaten ten minste één toezichthoudende autoriteit instellen, maar hun de mogelijkheid laat om er meerdere in te stellen. Deze verordening verleent elke lidstaat dus een beoordelingsmarge waardoor hij zo veel toezichthoudende autoriteiten kan instellen als nodig is, met name vanwege zijn constitutionele structuur.

---

[115] Respectievelijk artikel 55, lid 1, en artikel 77, lid 1, AVG.
[116] Op grond van artikel 51, lid 1, AVG.

Bovendien kan het feit dat een lidstaat zich beroept op bepalingen van nationaal recht niet afdoen aan de eenheid en de werking van het Unierecht. De gevolgen van het beginsel van voorrang van het Unierecht zijn immers bindend voor alle organen van een lidstaat; nationale bepalingen, waaronder ook constitutionele bepalingen, kunnen daar niet aan in de weg staan.

Wanneer een lidstaat ervoor heeft gekozen om één enkele toezichthoudende autoriteit in te stellen, kan hij zich dus niet beroepen op bepalingen van nationaal recht, ook niet van constitutionele aard, om onder de AVG vallende verwerkingen van persoonsgegevens aan het toezicht van deze autoriteit te onttrekken.

4. Voorwaarden voor het opleggen van administratieve geldboeten

Arrest van 5 december 2023 (Grote kamer), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

In deze zaak (zie tevens de rubrieken I.3., „Begrip ‚verwerking van persoonsgegevens'", I.5. „Begrip „‚voor de verwerking van persoonsgegevens verantwoordelijke'" en I.6, „Begrip ‚gezamenlijke verwerkingsverantwoordelijke'"), stelt het Hof vast dat er op grond van artikel 83 AVG alleen een administratieve geldboete kan worden opgelegd aan een verwerkingsverantwoordelijke indien vaststaat dat hij opzettelijk of uit nalatigheid inbreuk op de regels van deze verordening heeft gemaakt[117].

In dit verband preciseert het dat de Uniewetgever de lidstaten geen beoordelingsmarge heeft gelaten met betrekking tot de materiële voorwaarden waaraan een toezichthoudende autoriteit moet voldoen wanneer zij besluit om op grond van deze bepaling een administratieve geldboete op te leggen aan een verwerkingsverantwoordelijke. Het feit dat de AVG de lidstaten de mogelijkheid biedt om te voorzien in uitzonderingen met betrekking tot in die lidstaten gevestigde overheidsinstanties en overheidsorganen[118] alsook in eisen betreffende de procedure die de toezichthoudende autoriteiten moeten volgen om een administratieve geldboete op te leggen[119], betekent geenszins dat deze lidstaten ook bevoegd zijn om dergelijke materiële voorwaarden vast te stellen.

Wat deze voorwaarden betreft, merkt het Hof op dat één van de in de AVG opgesomde elementen – op basis waarvan de toezichthoudende autoriteit aan de verwerkingsverantwoordelijke een administratieve geldboete oplegt – „de opzettelijke of nalatige aard van de inbreuk"[120] is. Daarentegen is er bij geen van die factoren sprake van welke mogelijkheid ook om de verwerkingsverantwoordelijke aansprakelijk te

---

117 Inbreuk als bedoeld in artikel 83, leden 4-6.

118 Krachtens artikel 83, lid 7, AVG, dat bepaalt dat „elke lidstaat regels [kan] vaststellen betreffende de vraag of en in hoeverre administratieve geldboeten kunnen worden opgelegd aan in die lidstaat gevestigde overheidsinstanties en overheidsorganen".

119 Krachtens artikel 83, lid 8, AVG, gelezen in het licht van overweging 129 van die verordening.

120 Artikel 83, lid 2, onder b), AVG.

stellen wanneer hij geen fout heeft begaan. Bijgevolg kunnen alleen inbreuken op de AVG die de verwerkingsverantwoordelijke opzettelijk of uit nalatigheid heeft begaan ertoe leiden dat hem op grond van artikel 83 van die verordening een administratieve geldboete wordt opgelegd.

Het Hof voegt daaraan toe dat deze lezing steun vindt in de algemene opzet en het doel van de AVG. In dit verband vormt het bestaan van een sanctieregeling op grond waarvan krachtens de AVG een administratieve geldboete kan worden opgelegd indien de specifieke omstandigheden van elk geval dit rechtvaardigen, een stimulans voor de verwerkingsverantwoordelijken en verwerkers om deze verordening na te leven. Door hun afschrikkende werking dragen administratieve geldboeten bij tot een betere bescherming van de betrokken natuurlijke personen. De Uniewetgever heeft het echter niet noodzakelijk geacht om te voorzien in de oplegging van administratieve geldboeten als er geen sprake is van schuld. Aangezien de AVG tot doel heeft een gelijkwaardig en homogeen beschermingsniveau tot stand te brengen en deze verordening daartoe in de gehele Unie op coherente wijze moet worden toegepast, zou het in strijd zijn met dit doel als de lidstaten een dergelijke boeteregeling konden invoeren.

Tot slot oordeelt het Hof dat die geldboete kan worden opgelegd aan een verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens die door een verwerker namens hem wordt verricht, tenzij de verwerker in het kader van die verwerkingen de gegevens voor eigen doeleinden heeft verwerkt of op een wijze die onverenigbaar is met het kader of de wijze van verwerking zoals die door de verwerkingsverantwoordelijke waren bepaald of op zodanige wijze dat redelijkerwijs niet kan worden aangenomen dat de verwerkingsverantwoordelijke daarmee zou hebben ingestemd. In dat geval moet de verwerker worden geacht voor een dergelijke verwerking verantwoordelijk te zijn.

Arrest van 5 december 2023 (Grote kamer), Deutsche Wohnen (C-807/21, EU:C:2023:950)

Deutsche Wohnen SE (hierna: „DW") is een vastgoedvennootschap die indirect – via deelnemingen in verschillende vennootschappen – tal van commerciële en wooneenheden bezit. In het kader van haar commerciële activiteiten verwerkt zij persoonsgegevens van de huurders van deze eenheden.

Naar aanleiding van controles die zijn uitgevoerd in 2017 en 2019, heeft de Berliner Beauftragte für den Datenschutz (toezichthoudende autoriteit voor gegevensbescherming Berlijn, Duitsland) vastgesteld dat DW een reeks inbreuken op de AVG had begaan. Bij besluit van 30 oktober 2019 heeft deze toezichthoudende autoriteit haar dan ook administratieve geldboeten opgelegd.

DW heeft tegen dat besluit beroep ingesteld bij het Landgericht Berlin (rechter in eerste aanleg Berlijn, Duitsland), dat de procedure heeft stopgezet. Die rechter heeft

opgemerkt dat volgens de Duitse wet[121] een bestuursrechtelijk te bestraffen gedraging enkel kan worden geconstateerd jegens een natuurlijke persoon en niet jegens een rechtspersoon. Wanneer een rechtspersoon aansprakelijk wordt gesteld, kunnen hem bovendien alleen handelingen van de leden van zijn organen of van zijn vertegenwoordigers worden toegerekend. De Staatsanwaltschaft Berlin (openbaar ministerie Berlijn, Duitsland) heeft tegen die beslissing hoger beroep ingesteld bij het Kammergericht Berlin (hoogste rechterlijke instantie van de deelstaat Berlijn, Duitsland). In dit verband heeft die rechter het Hof verzocht om een prejudiciële beslissing over de uitlegging van de AVG.

In zijn arrest spreekt het Hof (Grote kamer) zich uit over de voorwaarden voor het opleggen van administratieve geldboeten op grond van de AVG. In de eerste plaats onderzoekt het Hof of de lidstaten de oplegging van een administratieve geldboete aan een rechtspersoon afhankelijk kunnen stellen van de voorwaarde dat de inbreuk op die verordening voorafgaandelijk is toegerekend aan een geïdentificeerde natuurlijke persoon. In de tweede plaats buigt het Hof zich, net als in het arrest Nacionalinis visuomenės sveikatos centras (zie hierboven), eveneens over de vraag of de bestrafte inbreuk op de bepalingen van de AVG opzettelijk dan wel uit nalatigheid moet zijn begaan.

Wat de oplegging van een administratieve geldboete aan een rechtspersoon op grond van de AVG betreft, merkt het Hof om te beginnen op dat de in de AVG neergelegde beginselen, verboden en verplichtingen in het bijzonder gericht zijn tot de „verwerkingsverantwoordelijken”, die verantwoordelijk zijn voor elke door of namens hen uitgevoerde verwerking van persoonsgegevens. Deze verantwoordelijkheid vormt, wanneer bepalingen van de AVG zijn geschonden, de grondslag voor de oplegging van een administratieve geldboete aan de verwerkingsverantwoordelijke op grond van artikel 83 van deze verordening. De Uniewetgever heeft bij de vaststelling van die verantwoordelijkheid evenwel geen onderscheid gemaakt tussen natuurlijke personen en rechtspersonen, aangezien voor die verantwoordelijkheid als enige voorwaarde geldt dat die personen, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststellen.[122] In beginsel is dus iedere persoon die aan deze voorwaarde voldoet, aansprakelijk voor elke inbreuk op de AVG die door hem of voor zijn rekening is begaan. Dit houdt om te beginnen in dat rechtspersonen niet alleen aansprakelijk zijn voor inbreuken die worden begaan door hun vertegenwoordigers, directeuren of beheerders, maar ook voor de inbreuken die worden begaan door iedere andere persoon die in het kader van de handelsactiviteiten van die rechtspersonen en voor hun rekening optreden. Daarnaast moeten de administratieve geldboeten waarin de AVG voor dergelijke inbreuken voorziet, rechtstreeks aan rechtspersonen kunnen worden opgelegd wanneer deze kunnen worden aangemerkt als verwerkingsverantwoordelijke.

---

[121] Gesetz über Ordnungswidrigkeiten (wet betreffende bestuursrechtelijk te bestraffen gedragingen) van 24 mei 1968 (BGBl. 1968 I, blz. 481), in de op 19 februari 1987 bekendgemaakte versie ervan (BGBl. 1987 I, blz. 602), zoals gewijzigd bij wet van 19 juni 2020 (BGBl. 2020 I, blz. 1350).

[122] Volgens artikel 4, punt 7, AVG.

Vervolgens merkt het Hof op dat uit geen enkele bepaling van de AVG kan worden afgeleid dat voor de oplegging van een administratieve geldboete aan een rechtspersoon als verwerkingsverantwoordelijke de voorwaarde geldt dat voorafgaandelijk is geconstateerd dat de inbreuk in kwestie is begaan door een geïdentificeerde natuurlijke persoon. Bovendien heeft de Uniewetgever de lidstaten op dit gebied geen beoordelingsruimte gelaten. Dat de AVG hun de mogelijkheid biedt om eisen te stellen aan de procedure die de toezichthoudende autoriteiten moeten volgen om een administratieve geldboete op te leggen[123], betekent geenszins dat zij ook bevoegd zijn om aanvullende materiële voorwaarden vast te stellen naast de materiële voorwaarden die zijn neergelegd in de AVG.

In dit verband verduidelijkt het Hof dat het in strijd met de doelstelling van de AVG zou zijn dat het de lidstaten werd toegestaan om eenzijdig als noodzakelijke voorwaarde voor de oplegging van een administratieve geldboete op grond van artikel 83 AVG aan een verwerkingsverantwoordelijke die een rechtspersoon is, te eisen dat de inbreuk in kwestie vooraf wordt toegerekend of kan worden toegerekend aan een geïdentificeerde natuurlijke persoon. Bovendien zou een dergelijk aanvullend vereiste uiteindelijk afbreuk dreigen te doen aan de doeltreffendheid en de afschrikkende werking van administratieve geldboeten die worden opgelegd aan rechtspersonen als verwerkingsverantwoordelijken.

Ten slotte beklemtoont het Hof dat het begrip „onderneming” in de zin van de artikelen 101 en 102 VWEU[124] geen invloed heeft op de beantwoording van de vraag of en onder welke voorwaarden op grond van de AVG een administratieve geldboete kan worden opgelegd aan een verwerkingsverantwoordelijke die een rechtspersoon is, en dat dit begrip enkel relevant is voor de vaststelling van het bedrag van een dergelijke geldboete.

Het Hof komt dan ook tot de slotsom dat de AVG[125] zich verzet tegen een nationale regeling op grond waarvan aan een rechtspersoon in zijn hoedanigheid van verwerkingsverantwoordelijke wegens een inbreuk op die verordening[126] alleen een administratieve geldboete kan worden opgelegd indien deze inbreuk vooraf is toegerekend aan een geïdentificeerde natuurlijke persoon.

Wat betreft de vraag of de lidstaten de oplegging van een administratieve geldboete ook mogelijk kunnen maken wanneer de bestrafte inbreuk niet opzettelijk of uit nalatigheid is begaan, brengt het Hof om te beginnen in herinnering dat de materiële voorwaarden die een toezichthoudende autoriteit in acht moet nemen wanneer zij een administratieve geldboete oplegt aan een verwerkingsverantwoordelijke, uitsluitend onder het Unierecht vallen en dat de lidstaten op dat gebied geen enkele beoordelingsruimte hebben. Het Hof stelt, in navolging van de door hem gevolgde redenering in het eerder genoemde arrest Nacionalinis visuomenės sveikatos centras,

---

123 Dit blijkt uit artikel 58, lid 4, en artikel 83, lid 8, AVG, gelezen in het licht van overweging 129 van deze verordening.
124 Naar dat begrip wordt verwezen in overweging 150 van de AVG.
125 Artikel 58, lid 2, onder i), en artikel 83, leden 1 tot en met 6, AVG.
126 Als bedoeld in artikel 83, leden 4 tot en met 6, AVG.

vast dat krachtens artikel 83 AVG slechts een administratieve geldboete kan worden opgelegd indien vaststaat dat de verwerkingsverantwoordelijke, die zowel een rechtspersoon als een onderneming is, opzettelijk of uit nalatigheid de regels van die verordening heeft geschonden.

5. Verhouding tussen de bevoegdheden van de nationale toezichthoudende autoriteiten en de bevoegdheden van de andere nationale autoriteiten

Arrest van 4 juli 2023 (Grote kamer), Meta Platforms e.a. (Algemene gebruiksvoorwaarden van een sociaal netwerk) (C-252/21, EU:C:2023:537)

In deze zaak (zie tevens rubriek V.5., „Verwerking van persoonsgegevens op online sociale netwerken"), waarin het Hof zich uitspreekt over de bevoegdheid van een mededingingsautoriteit om vast te stellen dat een verwerking van persoonsgegevens onverenigbaar is met de AVG, merkt het Hof op dat een dergelijke autoriteit in het kader van het onderzoek of er sprake is van misbruik van een machtspositie door een onderneming[127] kan vaststellen dat de algemene gebruiksvoorwaarden die deze onderneming met betrekking tot de verwerking van persoonsgegevens heeft opgesteld, en de toepassing van die gebruiksvoorwaarden niet met die verordening in overeenstemming zijn, mits die vaststelling noodzakelijk is om een dergelijk misbruik aan te tonen en zij haar verplichting tot loyale samenwerking[128] met de toezichthoudende autoriteiten nakomt. Een mededingingsautoriteit die bij de vaststelling dat misbruik wordt gemaakt van een machtspositie constateert dat de AVG is geschonden, treedt echter niet in de plaats van de toezichthoudende autoriteiten.

Gelet op het beginsel van loyale samenwerking moeten de mededingingsautoriteiten, wanneer zij bij de uitoefening van hun bevoegdheden onderzoeken of een gedraging van een onderneming in overeenstemming is met de AVG, dus met elkaar overleggen en loyaal samenwerken met de betrokken nationale toezichthoudende autoriteiten of met de leidende toezichthoudende autoriteit. Al deze autoriteiten moeten elkaars bevoegdheden en competenties op zodanige wijze eerbiedigen dat de verplichtingen die voortvloeien uit de AVG en de doelstellingen van deze verordening in acht worden genomen en het nuttig effect ervan wordt gewaarborgd. Hieruit volgt dat een mededingingsautoriteit die in het kader van het onderzoek naar misbruik van een machtspositie door een onderneming, van mening is dat moet worden geverifieerd of een gedraging van die onderneming in overeenstemming is met de AVG, moet nagaan of de bevoegde nationale toezichthoudende autoriteit, de leidende toezichthoudende autoriteit of het Hof reeds een besluit respectievelijk een beslissing heeft genomen over die of een soortgelijke gedraging. Indien dat het geval is, mag de mededingingsautoriteit

---

127 In de zin van artikel 102 VWEU.

128 Zoals vastgelegd in artikel 4, lid 3, VEU.

daar niet van afwijken, maar kan zij daar wel haar eigen conclusies aan verbinden voor de toepassing van het mededingingsrecht.

Wanneer de mededingingsautoriteit twijfels heeft over de draagwijdte van de beoordeling die door de bevoegde nationale toezichthoudende autoriteit of de leidende toezichthoudende autoriteit is gemaakt, wanneer de betrokken gedraging of een soortgelijke gedraging tegelijkertijd door deze autoriteiten wordt onderzocht, of wanneer die autoriteiten geen onderzoek hebben gedaan en de mededingingsautoriteit van mening is dat een gedraging van een onderneming niet in overeenstemming is met de AVG, moet zij deze autoriteiten raadplegen en om hun medewerking verzoeken, teneinde haar twijfels weg te nemen dan wel te bepalen of zij moet wachten tot de betrokken toezichthoudende autoriteit een besluit vaststelt alvorens met haar eigen beoordeling te beginnen. Indien de toezichthoudende autoriteiten niet binnen een redelijke termijn bezwaar maken of antwoorden, kan de mededingingsautoriteit haar eigen onderzoek voortzetten.

HOF VAN JUSTITIE
VAN DE EUROPESE UNIE

Directie Onderzoek en Documentatie

Juli 2024