boringen en fresingen standaard, en dus geen probleem zou zijn. De consument heeft dan niet heeft gekregen wat hij op grond van de overeenkomst mocht verwachten, hetgeen recht geeft op kosteloze vervanging of herstel op grond van artikel 7:17 jo. artikel 7:21 BW.[3]
Als laatste noem ik nog de mogelijkheid tot vernietiging op grond van dwaling, omdat de verkoper de consument over de plaatsing van de boor- en freesgaten had behoren in te lichten (artikel 6:228 lid 1 sub b BW). Nu het gaat om een expliciete dwingendrechtelijke informatieplicht kan niet aan de consument worden tegengeworpen dat deze daar zelf navraag naar had moeten doen.

4. Wat betreft de sancties bij de schending van informatieplichten bepaalt de aan afdeling 6.5.2B BW ten grondslag liggende Richtlijn consumentenrechten dat het aan de lidstaten is om sancties vast te stellen die 'doeltreffend, evenredig en afschrikkend' zijn.[4] Een vergelijkbare eis stelt Richtlijn 2008/48/EG (consumentenkrediet). In dat kader heeft het HvJ geoordeeld dat indien bij het aangaan van een kredietovereenkomst informatie wordt weggelaten die ertoe kan leiden dat de consument niet kan beoordelen waartoe hij zich heeft verbonden (ofwel informatie van essentieel belang) een evenredige sanctie kan zijn dat het krediet geacht wordt te zijn verstrekt zonder rente en kosten.[5] Het type informatieplicht dat wordt geschonden is dus relevant voor de vaststelling van de sanctie. Bij het schenden van informatieplichten die zien op naam en adresgegevens is een dergelijke vergaande sanctie niet evenredig. Informatie over voorname kenmerken van het product is evenwel zonder meer essentiële informatie, die een vergaande sanctie zoals nietigheid of gedeeltelijke nietigheid rechtvaardigt.
Ook informatie over het herroepingsrecht kan waarschijnlijk gezien worden als informatie die van essentieel belang is. In *Martin Martin* ging het om de schending van de informatieplichten over het bestaan van het herroepingsrecht en de voorwaarden waaronder dit recht kon worden uitgeoefend in het kader van colportage (Richtlijn 85/577/EEG). Het HvJ oordeelt in deze zaak eveneens dat als het de niet-nakoming van een verplichting betreft die essentieel is voor de wilsvorming van een consument, nietigheid van de overeenkomst een passende sanctie kan zijn.[6]

5. Terug naar het herroepingsrecht bij de online bestelde deuren. Het is maar zeer de vraag of het in het voorliggende geval gaat om zaken die volgens de specificaties van de consument zijn vervaardigd als bedoeld in artikel 6:230p sub f onder 1 BW. Volgens de memorie van toelichting bij de Implementatiewet richtlijn consumentenrechten is er geen sprake van een volgens opgave van de consument vervaardigde zaak indien de consument de keuze heeft uit een aantal standaardmaten.[7] Voor deuren gelden standaardmaten. Doorgaans zal de consument bij het online bestellen van een deur via een uitklapmenu uit bepaalde standaardmaten kunnen kiezen. Dan heeft de consument op grond van artikel 6:230o BW wel een herroepingsrecht binnen de bedenktijd.
Ten aanzien van het niet informeren over het bestaan van dit herroepingsrecht (of zelfs ten onrechte vermelden dat er geen herroepingsrecht is), is er een specifieke sanctie opgenomen in artikel 6:230o lid 2 BW. De bedenktijd wordt dan verlengd met de tijd die is verstreken tot het moment dat de informatie alsnog correct verstrekt is, tot maximaal twaalf maanden.

Mw. mr. dr. M.Y. Schaub

Privacy

HvJ EU 19 oktober 2016
(M. Ilešič, A. Prechal, A. Rosas, C. Toader en E. Jarašiūnas)
C-582/14
(Breyer/Duitsland)
(Zie de noot onder deze uitspraak.)

- *privacy*
- *persoonsgegevens*
- *consumentenbescherming*

Hoofdgeding en prejudiciële vragen

13. Breyer heeft verschillende websites van Duitse federale instellingen bezocht. Op deze voor het publiek toegankelijke sites stellen deze instellingen actuele informatie ter beschikking.

14. Teneinde cyberaanvallen af te weren en strafvervolging van de aanvallers mogelijk te maken, wordt bij de meeste van deze sites elk bezoek in logbestanden geregistreerd. In deze logbestanden worden na afloop van het bezoek van die sites de volgende gegevens bewaard: de naam van de opgevraagde website of van het opgevraagde bestand, de termen die in de zoekvelden werden ingevoerd, het tijdstip van de opvraging, de hoeveelheid overgedragen gegevens, het bericht of de opvraging is gelukt, en het IP-adres van de computer van waaraf de opvraging heeft plaatsgevonden.

3. Vergelijk Tussenadvies van de Geschillencommissie Thuiswinkel, THU09-0102.
4. Artikel 24 Richtlijn 2011/83/EU.
5. De kredietovereenkomst wordt dan in wezen deels als nietig aangemerkt, zie HvJ EU 9 november 2016, C-42/15, r.o. 71 (*Home Credit Slovakia*).
6. HvJ EU 17 december 2009, C-227/08, r.o. 34 (*Martin Martin*).
7. *Kamerstukken II* 2012/13, 33520, 3, p. 40.

15. IP-adressen zijn numerieke reeksen die worden toegekend aan computers die met het internet zijn verbonden, teneinde hun onderlinge communicatie via het internet mogelijk te maken. Als een website wordt bezocht, wordt het IP-adres van de computer waarmee de gegevens worden opgevraagd, doorgegeven aan de server waar de bezochte website is opgeslagen. Dit is nodig om de opgevraagde gegevens aan de juiste ontvanger over te dragen.

16. Voorts blijkt uit de verwijzingsbeslissing en uit het dossier waarover het Hof beschikt, dat internetproviders aan de computers van internetgebruikers ofwel een 'statisch' IP-adres toekennen, ofwel een 'dynamisch' IP-adres, dat wil zeggen een IP-adres dat bij elke nieuwe verbinding met het internet wijzigt. Anders dan statische IP-adressen maken dynamische IP-adressen het 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.

17. Breyer heeft bij de Duitse bestuursrechtelijke gerechten een beroep ingesteld dat ertoe strekt dat aan de Bondsrepubliek Duitsland een verbod wordt opgelegd om, na zijn bezoek van voor het publiek toegankelijke websites voor onlinemedia van Duitse federale instellingen, het IP-adres van zijn hostsysteem van waaraf de toegang tot deze websites heeft plaatsgevonden, te bewaren of door derden te doen bewaren, voor zover de bewaring van dat IP-adres niet nodig is om de beschikbaarheid van die media te herstellen in geval van storing.

18. Na de verwerping van zijn beroep in eerste aanleg heeft Breyer tegen de afwijzende beslissing hoger beroep ingesteld.

19. De appelrechter heeft deze beslissing gedeeltelijk hervormd. Hij heeft de Bondsrepubliek Duitsland gelast zich te onthouden van het na afloop van de desbetreffende sessie bewaren of door derden doen bewaren van het IP-adres van het hostsysteem van Breyer van waaraf de toegang heeft plaatsgevonden – welk IP-adres wordt doorgegeven telkens als Breyer voor het publiek toegankelijke websites voor onlinemedia van Duitse federale instellingen bezoekt – indien dit adres wordt bewaard samen met het tijdstip van het bezoek dat via dit adres heeft plaatsgevonden, en Breyer tijdens dit bezoek zijn identiteit heeft bekendgemaakt, onder meer in de vorm van een e-mailadres waaruit zijn identiteit blijkt, tenzij de bewaring van het IP-adres nodig is om de beschikbaarheid van het betrokken onlinemedium te herstellen in geval van storing.

20. Volgens de appelrechter vormt een dynamisch IP-adres samen met het tijdstip van het bezoek dat via dit adres heeft plaatsgevonden, een persoonsgegeven indien de gebruiker van de website in kwestie tijdens dit bezoek zijn identiteit heeft bekendgemaakt, aangezien de exploitant van deze site deze gebruiker kan identificeren door de naam van laatstgenoemde en het IP-adres van diens computer aan elkaar te koppelen.

21. De appelrechter heeft geoordeeld dat Breyers beroep evenwel niet dient te worden toegewezen in andere gevallen. Indien Breyer zijn identiteit tijdens een sessie niet bekendmaakt, dan kan namelijk enkel de internetprovider het IP-adres relateren aan de houder van een bepaalde aansluiting. Wanneer de Bondsrepubliek Duitsland als aanbieder van onlinemediadiensten de beschikking over het IP-adres krijgt, is dit adres daarentegen geen persoonsgegeven, zelfs niet samen met het tijdstip van het bezoek dat via dit adres heeft plaatsgevonden, aangezien de gebruiker van de betrokken websites niet door die lidstaat kan worden geïdentificeerd.

22. Zowel Breyer als de Bondsrepubliek Duitsland heeft bij het Bundesgerichtshof (hoogste federale rechter in burgerlijke en strafzaken, Duitsland) een beroep in 'Revision' ingesteld tegen de beslissing van de appelrechter. Breyer verzoekt dat zijn verbodsvordering integraal wordt toegewezen. De Bondsrepubliek Duitsland concludeert tot afwijzing van deze vordering.

23. De verwijzende rechter preciseert dat de dynamische IP-adressen van Breyers computer, die door de Bondsrepubliek Duitsland als aanbieder van onlinemediadiensten worden bewaard, althans in verband met de overige in de logbestanden opgeslagen gegevens, specifieke gegevens over zakelijke omstandigheden van Breyer vormen, aangezien zij informatie verstrekken over het feit dat Breyer via het internet op bepaalde tijdstippen bepaalde sites of bestanden heeft opgevraagd.

24. Aan de hand van de aldus bewaarde gegevens kan Breyers identiteit evenwel niet rechtstreeks worden achterhaald. De exploitanten van de in het hoofdgeding aan de orde zijnde websites kunnen Breyer immers alleen identificeren indien zij van zijn internetprovider informatie ontvangen over de identiteit van deze gebruiker. Deze gegevens kunnen dus enkel als 'persoonsgegevens' worden aangemerkt indien Breyer identificeerbaar was.

25. Het Bundesgerichtshof merkt op dat het in de rechtsleer omstreden is of een 'objectief' dan wel een 'relatief' criterium moet worden aangelegd om vast te stellen of iemand identificeerbaar is. De toepassing van een 'objectief' criterium heeft tot gevolg dat gegevens als de in het hoofdgeding aan de orde zijnde IP-adressen na afloop van het bezoek van de betrokken websites kunnen worden geacht persoonsgegevens te vormen, zelfs indien enkel een derde in staat is de identiteit van de betrokkene te achterhalen. Deze derde is in casu Breyers internetprovider, die extra gegevens heeft bewaard aan de hand waarvan Breyer via die IP-adressen kan worden geïdentificeerd. Indien een 'relatief' criterium wordt aangelegd, kunnen gegevens als de in het hoofdgeding aan de orde zijnde IP-adressen worden geacht persoonsgegevens te vormen ten aanzien van een lichaam als Breyers internetprovider, aangezien zij de precieze identificatie van de gebruiker mogelijk maken (zie dienaangaande arrest van 24 november 2011, Scarlet Extended, C-70/10, ECLI:EU:C:2011:771, punt 51), maar zouden zij niet kunnen worden geacht persoonsgegevens te vormen ten aanzien van een ander lichaam, zoals de exploitant van de door Breyer bezochte websites, aangezien deze exploi-

tant – in de veronderstelling dat Breyer zijn identiteit niet heeft bekendgemaakt tijdens het bezoek van deze sites – niet beschikt over de informatie die nodig is om Breyer zonder excessieve inspanning te identificeren.

26. Voor het geval dat de dynamische IP-adressen van Breyers computer, samen met het tijdstip van de desbetreffende sessie, moeten worden geacht persoonsgegevens te vormen, wenst de verwijzende rechter te vernemen of de bewaring van deze IP-adressen na afloop van deze sessie is toegestaan op grond van artikel 7, onder f), van richtlijn 95/46.

27. In dit verband zet het Bundesgerichtshof om te beginnen uiteen dat aanbieders van onlinemediadiensten volgens § 15, lid 1, TMG persoonsgegevens van een gebruiker enkel mogen verzamelen en benutten voor zover dit noodzakelijk is om het gebruik van onlinemedia mogelijk te maken en te factureren. Voorts merkt de verwijzende rechter op dat het volgens de Bondsrepubliek Duitsland nodig is deze gegevens te bewaren om de veiligheid en de goede werking van websites voor onlinemediadiensten die zij toegankelijk maakt voor het publiek, te waarborgen en in stand te houden. De bewaring van die gegevens maakt het namelijk in het bijzonder mogelijk 'denial-of-serviceaanvallen' te herkennen en te bestrijden, dat wil zeggen cyberaanvallen die tot doel hebben de werking van deze sites te ontwrichten door het gericht en gecoördineerd bestoken van bepaalde internetservers met een groot aantal aanvragen.

28. Indien en voor zover het nodig is dat de aanbieder van onlinemediadiensten maatregelen treft om dergelijke aanvallen te bestrijden, kunnen deze maatregelen volgens de verwijzende rechter noodzakelijk worden geacht om 'het gebruik van onlinemedia mogelijk te maken' in de zin van § 15 TMG. In de rechtsleer wordt evenwel voornamelijk de opvatting gehuldigd dat het verzamelen en benutten van persoonsgegevens van gebruikers van een website enkel geoorloofd is om een concreet gebruik van deze site mogelijk te maken, en dat deze gegevens na de desbetreffende sessie moeten worden uitgewist indien zij niet vereist zijn voor factureringsdoeleinden. Een dergelijke restrictieve lezing van § 15, lid 1, TMG staat er volgens de verwijzende rechter aan in de weg dat IP-adressen worden bewaard om de veiligheid en de goede werking van onlinemedia in het algemeen te waarborgen en in stand te houden.

29. De verwijzende rechter vraagt zich af of deze – door de appelrechter voorgestane – uitlegging strookt met artikel 7, onder f), van richtlijn 95/46, met name gelet op de criteria die het Hof heeft ontwikkeld in de punten 29 en volgende van het arrest van 24 november 2011, ASNEF en FECEMD (C-468/10 en C-469/10, ECLI:EU:C:2011:777).

30. Het Bundesgerichtshof heeft de behandeling van de zaak dan ook geschorst en het Hof verzocht om een prejudiciële beslissing over de volgende vragen:
'1) Dient artikel 2, onder a), van richtlijn 95/46 aldus te worden uitgelegd dat een internetprotocoladres (IP-adres) dat een aanbieder van [onlinemedia]diensten opslaat wanneer zijn internetsite wordt bezocht, voor deze aanbieder reeds dan een persoonsgegeven vormt, wanneer een derde (in casu: de internetprovider) beschikt over de aanvullende gegevens die nodig zijn om de betrokken persoon te identificeren?
2) Verzet artikel 7, onder f), van [deze richtlijn] zich tegen een regel van nationaal recht op grond waarvan de aanbieder van [onlinemedia]diensten 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]?'

Prejudiciële vragen

Eerste prejudiciële vraag

31. Met zijn eerste vraag wenst de verwijzende rechter in wezen te vernemen of artikel 2, onder a), van richtlijn 95/46 aldus moet worden uitgelegd dat een dynamisch IP-adres dat door een aanbieder van onlinemediadiensten wordt geregistreerd telkens als 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 voormelde bepaling vormt, wanneer enkel een derde, in casu de internetprovider van die persoon, beschikt over de extra informatie die nodig is om die persoon te identificeren.

32. In artikel 2, onder a), van richtlijn 95/46 worden 'persoonsgegevens' gedefinieerd als 'iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna "betrokkene" te noemen'. Op grond van deze bepaling wordt als identificeerbaar beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.

33. Vooraf zij opgemerkt dat het Hof in punt 51 van het arrest van 24 november 2011, Scarlet Extended (C-70/10, ECLI:EU:C:2011:771), dat onder meer betrekking had op de uitlegging van dezelfde richtlijn, in wezen heeft geoordeeld dat IP-adressen van internetgebruikers beschermde persoonsgegevens zijn, aangezien zij de precieze identificatie van deze gebruikers mogelijk maken.

34. Deze vaststelling van het Hof betrof evenwel het geval waarin IP-adressen van internetgebruikers worden verzameld en geïdentificeerd door de internetproviders.

35. In de onderhavige zaak betreft de eerste vraag daarentegen het geval waarin IP-adressen van gebruikers van een website die voor het publiek toegankelijk wordt gemaakt door de aanbieder van onlinemediadiensten, te weten de Bondsrepubliek Duitsland, worden geregistreerd door die aanbieder, zonder dat deze beschikt over de extra informatie die nodig is om die gebruikers te identificeren.

36. Voorts staat vast dat de IP-adressen waaraan de verwijzende rechter refereert, 'dynamische' IP-adressen zijn – dat wil zeggen tijdelijke IP-adressen die bij elke verbinding met het internet worden toegekend en bij latere verbindingen worden vervangen – en geen 'statische' IP-adressen, die onveranderlijk zijn en de permanente identificatie van het met het internet verbonden apparaat mogelijk maken.

37. De eerste vraag van de verwijzende rechter berust dus op de premisse dat, ten eerste, gegevens die bestaan in een IP-adres en de datum en het uur waarop een website via dit IP-adres is bezocht, zoals deze gegevens door een aanbieder van onlinemediadiensten zijn geregistreerd, op zichzelf deze aanbieder niet de mogelijkheid bieden om de gebruiker te identificeren die deze website tijdens de desbetreffende sessie heeft bezocht en, ten tweede, de internetprovider zijnerzijds beschikt over extra informatie die het mogelijk maakt, wanneer zij wordt gecombineerd met dat IP-adres, die gebruiker te identificeren.

38. In dit verband zij allereerst opgemerkt dat het vaststaat dat een dynamisch IP-adres geen gegeven vormt dat betrekking heeft op een 'geïdentificeerde (…) natuurlijke persoon', aangezien uit een dergelijk adres niet rechtstreeks blijkt welke de identiteit is van de natuurlijke persoon die eigenaar is van de computer van waaraf een website is bezocht, noch welke de identiteit is van een andere persoon die mogelijkerwijs van deze computer gebruikmaakt.

39. Om vast te stellen of een dynamisch IP-adres – in het in punt 37 van dit arrest uiteengezette geval – ten aanzien van een aanbieder van onlinemediadiensten een persoonsgegeven in de zin van artikel 2, onder a), van richtlijn 95/46 vormt, dient vervolgens te worden nagegaan of een dergelijk IP-adres dat door die aanbieder wordt geregistreerd, kan worden aangemerkt als een gegeven dat betrekking heeft op een 'identificeerbare natuurlijke persoon', wanneer de extra informatie die nodig is voor de identificatie van de gebruiker van een website die deze aanbieder toegankelijk maakt voor het publiek, bij de internetprovider van deze gebruiker berust.

40. Dienaangaande blijkt uit de bewoordingen van artikel 2, onder a), van richtlijn 95/46 dat een persoon niet alleen als identificeerbaar wordt beschouwd wanneer hij direct kan worden geïdentificeerd, maar ook wanneer hij indirect kan worden geïdentificeerd.

41. Uit het feit dat de Uniewetgever de uitdrukking 'indirect' gebruikt, kan worden afgeleid dat het voor de kwalificatie van een gegeven als persoonsgegeven niet nodig is dat dit gegeven het op zichzelf mogelijk maakt de betrokken persoon te identificeren.

42. Bovendien moet volgens overweging 26 van richtlijn 95/46, om te bepalen of een persoon identificeerbaar is, worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is, dan wel door enige andere persoon, kunnen worden ingezet om voornoemde persoon te identificeren.

43. Aangezien deze overweging verwijst naar de middelen die redelijkerwijs kunnen worden ingezet door zowel de persoon die voor de verwerking verantwoordelijk is als een 'ander[e] persoon', kan uit de bewoordingen ervan worden opgemaakt dat het 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.

44. 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.

45. Vastgesteld dient evenwel te worden of de mogelijkheid om een dynamisch IP-adres te combineren met de extra informatie waarvan die internetprovider in het bezit is, een middel vormt waarvan mag worden aangenomen dat het redelijkerwijs kan worden ingezet om de betrokken persoon te identificeren.

46. Zoals de advocaat-generaal in punt 68 van zijn conclusie in wezen heeft opgemerkt, is dit niet het geval indien de identificatie van de betrokkene bij de wet verboden wordt of in de praktijk ondoenlijk is, bijvoorbeeld omdat zij – gelet op de vereiste tijd, kosten en mankracht – een excessieve inspanning vergt, zodat het gevaar voor identificatie in werkelijkheid onbeduidend lijkt.

47. Hoewel de verwijzende rechter in zijn verwijzingsbeslissing preciseert dat de internetprovider de extra informatie die noodzakelijk is voor de identificatie van de betrokken persoon, naar Duits recht niet rechtstreeks mag doorgeven aan de aanbieder van onlinemediadiensten, lijken er – onder voorbehoud van de door de verwijzende rechter in dit verband te verrichten verificaties – voor de aanbieder van onlinemediadiensten juridische mogelijkheden te bestaan om zich, met name in geval van cyberaanvallen, te wenden tot de bevoegde autoriteit opdat deze de nodige stappen onderneemt om die informatie van de internetprovider te verkrijgen en om strafvervolging in te stellen.

48. De aanbieder van onlinemediadiensten lijkt dan ook te beschikken over middelen waarvan mag worden aangenomen dat zij redelijkerwijs kunnen worden ingezet om de betrokken persoon met behulp van derden, te weten de bevoegde autoriteit en de internetprovider, te identificeren aan de hand van de bewaarde IP-adressen.

49. Gelet op een en ander dient op de eerste vraag te worden geantwoord dat artikel 2, onder a), van richtlijn 95/46 aldus moet worden uitgelegd dat een dynamisch IP-adres dat door een aanbieder van onlinemediadiensten wordt geregistreerd telkens als een persoon een website bezoekt die door deze aanbieder toegankelijk wordt ge-

maakt voor het publiek, ten aanzien van die aanbieder een persoonsgegeven in de zin van voormelde bepaling vormt, wanneer hij beschikt over wettige middelen waarmee hij de betrokken persoon kan identificeren aan de hand van extra informatie die bij de internetprovider van deze persoon berust.

Tweede prejudiciële vraag

50. Met zijn tweede vraag wenst de verwijzende rechter in wezen te vernemen of artikel 7, onder f), van richtlijn 95/46 aldus moet worden uitgelegd dat het zich verzet tegen een regeling van een lidstaat op grond waarvan een aanbieder van onlinemediadiensten persoonsgegevens van een gebruiker van deze diensten zonder diens toestemming enkel mag verzamelen en benutten voor zover dit nodig is om het concrete gebruik van deze diensten door deze gebruiker mogelijk te maken en te factureren, zonder dat de doelstelling die erin bestaat de goede werking van die diensten in het algemeen te waarborgen, rechtvaardigt dat die gegevens worden benut na afloop van de desbetreffende sessie.

51. Aan de beantwoording van deze vraag dient de vaststelling vooraf te gaan of de verwerking van de in het hoofdgeding aan de orde zijnde persoonsgegevens, te weten de dynamische IP-adressen van de gebruikers van bepaalde websites van Duitse federale instellingen, niet van de werkingssfeer van richtlijn 95/46 is uitgesloten op grond van artikel 3, lid 2, eerste streepje, van deze richtlijn, dat bepaalt dat deze richtlijn niet van toepassing is op de verwerking van persoonsgegevens die betrekking hebben op – onder meer – de activiteiten van de staat op strafrechtelijk gebied.

52. In dit verband zij eraan herinnerd dat de activiteiten die in die bepaling als voorbeeld worden vermeld, in alle gevallen specifieke activiteiten van staten of overheidsinstanties betreffen die niets van doen hebben met de gebieden waarop particulieren activiteiten ontplooien (zie arresten van 6 november 2003, Lindqvist, C-101/01, ECLI:EU:C:2003:596, punt 43, en 16 december 2008, Satakunnan Markkinapörssi en Satamedia, C-73/03, ECLI:EU:C:2008:727, punt 41).

53. Onder voorbehoud van de door de verwijzende rechter ter zake te verrichten verificaties, lijken in het hoofdgeding de Duitse federale instellingen, die onlinemediadiensten aanbieden en die verantwoordelijk zijn voor de verwerking van de dynamische IP-adressen, ondanks hun status van overheidsinstantie als particulieren en niet in het kader van de activiteiten van de staat op strafrechtelijk gebied te handelen.

54. Derhalve dient te worden vastgesteld of een regeling van een lidstaat zoals de regeling die in het hoofdgeding aan de orde is, verenigbaar is met artikel 7, onder f), van richtlijn 95/46.

55. Daartoe zij eraan herinnerd dat de litigieuze nationale regeling – in de door de verwijzende rechter vermelde restrictieve uitlegging ervan – enkel toestaat dat persoonsgegevens van een gebruiker van onlinemediadiensten zonder diens toestemming worden verzameld en benut voor zover dit nodig is om het concrete gebruik van het betrokken onlinemedium door deze gebruiker mogelijk te maken en te factureren, zonder dat de doelstelling die erin bestaat de goede werking van dit medium in het algemeen te waarborgen, rechtvaardigt dat die gegevens worden gebruikt na afloop van de desbetreffende sessie.

56. Volgens artikel 7, onder f), van richtlijn 95/46 is de verwerking van persoonsgegevens 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 die aanspraak maakt op bescherming uit hoofde van artikel 1, lid 1, van deze richtlijn, niet prevaleren'.

57. In herinnering dient te worden gebracht dat het Hof heeft geoordeeld dat artikel 7 van richtlijn 95/46 een uitputtende lijst bevat van gevallen waarin een verwerking van persoonsgegevens als rechtmatig kan worden aangemerkt, en dat de lidstaten aan dit artikel geen nieuwe beginselen betreffende de toelaatbaarheid van de verwerking van persoonsgegevens mogen toevoegen, noch bijkomende vereisten mogen vaststellen die de reikwijdte van een van de zes in dat artikel vervatte beginselen zouden wijzigen (zie in die zin arrest van 24 november 2011, ASNEF en FECEMD, C-468/10 en C-469/10, ECLI:EU:C:2011:777, punten 30 en 32).

58. Weliswaar staat artikel 5 van richtlijn 95/46 de lidstaten toe om – binnen de grenzen van hoofdstuk II van deze richtlijn en dus binnen de grenzen van artikel 7 ervan – de voorwaarden nader te bepalen waaronder de verwerking van persoonsgegevens rechtmatig is, maar van de beoordelingsmarge waarover de lidstaten krachtens voornoemd artikel 5 beschikken, kan enkel worden gebruikgemaakt in overeenstemming met het doel van die richtlijn, dat erin bestaat een evenwicht tussen het vrije verkeer van persoonsgegevens en de bescherming van de persoonlijke levenssfeer te verzekeren. De lidstaten mogen krachtens artikel 5 van richtlijn 95/46 geen andere beginselen betreffende de toelaatbaarheid van de verwerking van persoonsgegevens invoeren dan die welke worden genoemd in artikel 7 van deze richtlijn, noch door middel van bijkomende vereisten de reikwijdte van de zes in laatstgenoemd artikel vervatte beginselen wijzigen (zie in die zin arrest van 24 november 2011, ASNEF en FECEMD, C-468/10 en C-469/10, ECLI:EU:C:2011:777, punten 33, 34 en 36).

59. In casu blijkt § 15 TMG – indien het wordt uitgelegd op de restrictieve wijze die in punt 55 van het onderhavige arrest is vermeld – een beperktere reikwijdte te hebben dan die van het in artikel 7, onder f), van richtlijn 95/46 vervatte beginsel.

60. Artikel 7, onder f), van deze richtlijn verwijst namelijk in het algemeen naar de 'behartiging van het gerechtvaardigde belang van de voor de verwerking verantwoordelijke of van de derde(n) aan wie de gegevens worden verstrekt', terwijl § 15 TMG de aanbieder van diensten uitsluitend toestaat persoonsgegevens van een gebruiker

te verzamelen en te benutten voor zover dit nodig is om het concrete gebruik van onlinemedia mogelijk te maken en te factureren. § 15 TMG verzet er zich dus in het algemeen tegen dat persoonsgegevens, nadat van onlinemediadiensten is gebruikgemaakt, worden bewaard om het gebruik van onlinemedia te garanderen. De Duitse federale instellingen die onlinemediadiensten aanbieden, zouden er evenwel ook een gerechtvaardigd belang bij kunnen hebben dat de goede werking van hun voor het publiek toegankelijke websites na elk concreet gebruik ervan in stand wordt gehouden.

61. Zoals de advocaat-generaal in de punten 100 en 101 van zijn conclusie heeft opgemerkt, wordt er in een dergelijke nationale regeling niet mee volstaan het in artikel 7, onder f), van richtlijn 95/46 gehanteerde begrip 'gerechtvaardigd belang' nader te bepalen overeenkomstig artikel 5 van deze richtlijn.

62. In dit verband zij er tevens aan herinnerd dat artikel 7, onder f), van richtlijn 95/46 zich ertegen verzet dat een lidstaat voor bepaalde categorieën persoonsgegevens categorisch en generiek de mogelijkheid van verwerking uitsluit, zonder ruimte te bieden voor een afweging van de betrokken tegengestelde rechten en belangen in een concreet geval. Een lidstaat mag voor deze categorieën de uitkomst van de afweging van de tegengestelde rechten en belangen dan ook niet definitief vaststellen, zonder ruimte te bieden voor een afwijkende uitkomst wegens de bijzondere omstandigheden van een concreet geval (zie in die zin arrest van 24 november 2011, ASNEF en FECEMD, C-468/10 en C-469/10, ECLI:EU:C:2011:777, punten 47-48).

63. Met betrekking tot de verwerking van persoonsgegevens van de gebruikers van websites voor onlinemedia beperkt een regeling als die welke in het hoofdgeding aan de orde is, de reikwijdte van het in artikel 7, onder f), van richtlijn 95/46 vervatte beginsel, doordat zij eraan in de weg staat dat de doelstelling de goede werking van het desbetreffende onlinemedium in het algemeen te waarborgen wordt afgewogen tegen het belang of de fundamentele rechten en vrijheden van die gebruikers, die overeenkomstig deze bepaling aanspraak maken op bescherming op grond van artikel 1, lid 1, van die richtlijn.

64. Gelet op een en ander dient op de tweede vraag te worden geantwoord dat artikel 7, onder f), van richtlijn 95/46 aldus moet worden uitgelegd dat het zich verzet tegen een regeling van een lidstaat op grond waarvan een aanbieder van onlinemediadiensten persoonsgegevens van een gebruiker van deze diensten zonder diens toestemming enkel mag verzamelen en benutten voor zover dit nodig is om het concrete gebruik van deze diensten door deze gebruiker mogelijk te maken en te factureren, zonder dat de doelstelling de goede werking van die diensten in het algemeen te waarborgen kan rechtvaardigen dat die gegevens worden gebruikt na afloop van de desbetreffende sessie.

Kosten

65. Ten aanzien van de partijen in het hoofdgeding is de procedure als een aldaar gerezen incident te beschouwen, zodat de verwijzende rechter over de kosten heeft te beslissen. De door anderen wegens indiening van hun opmerkingen bij het Hof gemaakte kosten komen niet voor vergoeding in aanmerking.

Het Hof (Tweede kamer) verklaart voor recht:
1) Artikel 2, onder a), van 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, moet aldus worden uitgelegd dat een dynamisch internetprotocoladres dat door een aanbieder van onlinemediadiensten wordt geregistreerd telkens als 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 voormelde bepaling vormt, wanneer hij beschikt over wettige middelen waarmee hij de betrokken persoon kan identificeren aan de hand van extra informatie die bij de internetprovider van deze persoon berust.
2) Artikel 7, onder f), van richtlijn 95/46 moet aldus worden uitgelegd dat het zich verzet tegen een regeling van een lidstaat op grond waarvan een aanbieder van onlinemediadiensten persoonsgegevens van een gebruiker van deze diensten zonder diens toestemming enkel mag verzamelen en benutten voor zover dit nodig is om het concrete gebruik van deze diensten door deze gebruiker mogelijk te maken en te factureren, zonder dat de doelstelling de goede werking van die diensten in het algemeen te waarborgen kan rechtvaardigen dat die gegevens worden gebruikt na afloop van de desbetreffende sessie.

NOOT

Het internet biedt vele gelegenheden om weer eens ten principale uit te zoeken hoe het staat met voor de hand liggende concepten. Zo vindt de communicatie op het internet veelal plaats via 'unieke' IP-adressen. Een gebruiker krijgt van zijn internettoegangsaanbieder een dergelijk adres toegekend, dat vervolgens de basis vormt voor de vindbaarheid van, communicatie met of herkenning van de gebruiker. Aldus spelen IP-adressen een rol bij marketingactiviteiten en het tot stand komen van transacties. Eigenlijk zijn er veel overeenkomsten met klassieke telefoonnummers of huisadressen. Echter, IP-adressen zijn niet altijd 'uniek', maar kunnen ook door de internettoegangsaanbieder op tijdelijke basis – voor de duur van een bezoek op het internet – worden toegekend. Men spreekt dan van dynamische IP-adressen. Deze zijn maar voor een bepaalde tijd 'uniek' en kunnen vervolgens weer aan een andere gebruiker worden toegekend.[1]

Vanuit het privacyrecht is er een bijzondere reden om duidelijkheid te krijgen over de status van IP-adressen,

1. Ook bij telefoonnummers en huisadressen is eigenlijk sprake van een vergelijkbare situatie: telefoonnummers kunnen vrijvallen en opnieuw worden uitgegeven. Huizen worden verlaten en krijgen nieuwe bewoners. De dynamiek van dynamische IP-adressen – de naam zegt het al – is natuurlijk wel anders.

en in het bijzonder deze dynamische IP-adressen.[2] Wanneer dynamische IP-adressen beschouwd kunnen worden als een persoonsgegeven, zijn op het gebruik ervan de strikte regels uit het privacyrecht van toepassing. Deze zijn met name neergelegd in twee richtlijnen, de Algemene privacyrichtlijn (Richtlijn 95/46/EG) en de e-Privacyrichtlijn (Richtlijn 2002/58/EG). De eerste richtlijn is inmiddels vervangen door de Algemene verordening gegevensbescherming (AVG, Verordening (EU) 2016/679), die vanaf 25 mei 2018 geldend recht wordt. Het is de bedoeling om de e-Privacyrichtlijn eveneens te vervangen door een verordening. Een voorstel daartoe is in behandeling.[3] Voor de zaak die hier aan de orde is, maakt het bestaan van de twee richtlijnen niet veel uit omdat ze gebaseerd zijn op hetzelfde begrippenkader.

De strikte privacyregels omvatten veel waarborgen die hun basis vinden in klassieke beginselen van het consumentenrecht. Daartoe behoren informatieverplichtingen, het in voorkomende gevallen daadwerkelijk verkrijgen van toestemming voor het gebruik en de verwerking van persoonsgegevens, waarborgen met betrekking tot de zorgvuldige omgang met en gebruik van de gegevens zoals de verstrekking ervan aan derden. Er staan dus grote belangen op het spel. Is een IP-adres geen persoonsgegeven, dan zijn de bijzondere privacyregels niet van toepassing.

Er is een duidelijke richtingenstrijd: aan de ene kant zijn er auteurs die hun bedenkingen hebben bij het automatisch als een persoonsgegeven bestempelen van een IP-adres. Zwenne geeft in zijn oratie *De verwaterde privacywet* een overzicht van de diverse opvattingen en betuigt zich geen voorstander van het al te gemakkelijk oprekken van het begrip 'persoonsgegevens'.[4] Anderzijds hebben de Europese privacytoezichthouders, verenigd in de zogenaamde Artikel 29-werkgroep, zich voor een meer open interpretatie uitgesproken.[5] Zuiderveen Borgesius zit op eenzelfde lijn.[6]

Het Hof van Justitie hakt nu de knoop door in een overzichtelijk arrest.[7] Het geeft een uitleg van de definitie van persoonsgegevens zoals neergelegd in artikel 2 onderdeel a van de Privacyrichtlijn, waarin wordt gesteld dat het bij persoonsgegevens gaat om 'iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna "betrokkene" te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit'.[8] De directe identificatie van een persoon aan de hand van een IP-adres is niet mogelijk, zoals het Hof ook al eerder vaststelde, maar naar de opvatting van het Hof kan er bij dynamische IP-adressen wel sprake zijn van een 'identificeerbaar natuurlijke persoon'.[9] Voor deze kwalificatie is van belang dat aan een redelijkheidstoets wordt voldaan, namelijk dat gekeken moet worden naar 'alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de werking verantwoordelijk is, dan wel door enige andere persoon, kunnen worden ingezet om voornoemde personen te identificeren'. Er mag geen excessieve inspanning worden verlangd om de identiteit te achterhalen.[10] In het concrete geval zou de onlinedienstenaanbieder in samenspraak met de bevoegde autoriteit en internetprovider in staat moeten zijn om de identiteit te achterhalen. Daarbij kunnen zich wel beperkingen voordoen, zoals een verbod met betrekking tot toegang of gebruik van gegevens. Dit vinden we dan ook terug in het finale oordeel van het Hof: 'Artikel 2, onder a), van 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, moet aldus worden uitgelegd dat een dynamisch internetprotocoladres dat door een aanbieder van onlinemediadiensten wordt geregistreerd telkens als 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 voormelde bepaling vormt, wanneer hij beschikt over wettige middelen waarmee hij de betrokken persoon kan identificeren aan de hand van extra informatie die bij de internetprovider van deze persoon berust.' De 'wettige middelen' geven hier deze beperking aan.

Het arrest geeft aanleiding tot ten minste twee observaties. In de eerste plaats zal door technologische en andere ontwikkelingen, zoals het steeds grootschaliger verzamelen van data, het steeds eenvoudiger worden om te spreken van situaties die conform het criterium van de richtlijn leiden tot het identificeren van personen. Enerzijds betekent dit goed nieuws: de betreffende personen kunnen aanspraak maken op de bescherming zoals neergelegd in de privacyregels. Anderzijds is dit slecht nieuws: de mogelijkheden om anoniem te zijn en blijven op het internet nemen verder af. Dit kan betekenen dat zoge-

2. Zie over privacy in relatie tot het consumentenrecht: F.J. Zuiderveen Borgesius, 'Privacy van consumenten', in: E.H. Hondius & G.J. Rijken (red.), *Handboek Consumentenrecht*, Zutphen: Uitgeverij Paris 2015, p. 483-497.
3. ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.
4. Zie zwenneblog.weblog.leidenuniv.nl/files/2013/09/G-J.-Zwenne-De-verwaterde-privacywet-oratie-Leiden-12-apri-2013-NED.pdf.
5. O.a. in: Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 01248/07/EN, WP 136, 20 juni 2007 (ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf).
6. F.J. Zuiderveen Borgesius, 'Mensen aanwijzen maar niet bij naam noemen: behavioural targeting, persoonsgegevens en de nieuwe Privacyverordening', *TvC* 2016, afl. 2, p. 54-66 (www.ivir.nl/publicaties/download/1786).
7. Het Hof oordeelde ook nog over een andere bepaling van de Privacyrichtlijn (artikel 7, onder f), waar het gaat om het verzamelen van gebruikersgegevens. Dit aspect blijft buiten deze bespreking van het arrest. Ook laten we het achterliggende feitencomplex hier onbesproken aangezien dit niet relevant is voor de in het geding zijnde rechtsvraag.
8. Aangezien de definitie van persoonsgegevens tussen de Privacyrichtlijn en de Algemene verordening gegevensbescherming (AVG) voor wat betreft het onderwerp van de zaak niet wezenlijk verschilt, zal het oordeel van het Hof relevant blijven na mei 2018.
9. R.o. 42.
10. R.o. 46.

naamde 'chilling effects' toenemen: gebruikers passen hun gedrag aan vanwege de vrees dat hun informatie wordt gebruikt voor zaken die zij niet wenselijk achten. Daarmee neemt de noodzaak toe om – als gebruiker en aanbieder – zorgvuldig te zijn met het gebruiken en delen van tot natuurlijke personen herleidbare gegevens. In andere uitspraken heeft het Hof al aangegeven dat het delen van gebruikersgegevens onderwerp moet zijn van een bredere belangenafweging, waarbij ook fundamentele rechten een rol moeten spelen.[11]

Een tweede observatie betreft de positie van natuurlijke personen vanuit een consumentenperspectief. De uitspraak maakt het privacyrecht nog verder deel van het recht dat door consumenten mogelijk kan worden ingeroepen ter bescherming van hun belangen. De vraag kan worden gesteld of dat wel de rol van het privacyrecht moet zijn c.q. hoe het privacyrecht zich verhoudt tot meer algemeen consumentenrecht dat vergelijkbare waarborgen biedt, zoals het recht met betrekking tot oneerlijke handelspraktijken.[12]

Prof. dr. N.A.N.M. van Eijk

Procesrecht

HvJ EU 28 juli 2016
(L. Bay Larsen, D. Švaby, J. Malenovský, M. Safjan en M. Vilaras)
C-191/15
(Verein für Konsumenteninformation/Amazon EU Sàrl)
(Zie de noot onder deze uitspraak.)

– *internationaal privaatrecht*
– *rechtskeuze*
– *consumentenrecht*

Hoofdgeding en prejudiciële vragen

29. Amazon EU is een in Luxemburg gevestigde vennootschap die deel uitmaakt van een internationale groep van postorderbedrijven. Naast andere activiteiten richt zij zich, via haar website met een domeinnaam en de extensie '.de', op in Oostenrijk woonachtige consumenten, met wie zij online verkoopovereenkomsten afsluit. Deze vennootschap heeft geen zetel of vestiging in Oostenrijk.

30. Tot medio 2012 luidden de in de met deze consumenten gesloten overeenkomsten opgenomen algemene voorwaarden als volgt:
'1. Afwijkende bedingen van de koper worden door Amazon.de niet aanvaard, tenzij Amazon.de hiermee uitdrukkelijk schriftelijk heeft ingestemd.
(…)
6. Bij koop op rekening alsmede in andere gevallen waarin daartoe een redelijke aanleiding bestaat, toetst en beoordeelt Amazon.de de door de koper opgegeven gegevens en wisselt informatie uit met andere ondernemingen binnen het Amazonconcern, handelsinformatiebureaus en eventueel Bürgel Wirtschaftsinformationen GmbH & Co, Postbus 5001 66, 22701, Hamburg, Duitsland.
(…)
9. Met het oog op de beslissing voor koop op rekening als betaalwijze gebruiken wij – naast onze eigen gegevens – voor de beoordeling van het kredietrisico waarschijnlijkheidswaarden die wij verwerven bij Bürgel Wirtschaftsinformationen GmbH & Co. KG, Gasstraße 18, 22761 Hamburg, en bij informa Solutions GmbH, Rheinstrasse 99, 76532, Baden-Baden [(Duitsland)]. Deze ondernemingen worden voorts ingeschakeld voor het valideren van de door u opgegeven adresgegevens.
(…)
11. Indien de gebruiker ervoor kiest om content (bijvoorbeeld klantrecensies) op Amazon.de te plaatsen, verleent hij Amazon een voor de duur van het onderliggende recht naar tijd en plaats onbeperkte licentie voor het verdere gebruik van de content, zowel online als offline en ongeacht voor welk doel.
12. Van toepassing is het Luxemburgse recht met uitsluiting van het verdrag der Verenigde Naties inzake internationale koopovereenkomsten betreffende roerende zaken (CISG).'

31. De VKI, een entiteit die bevoegd is om verbodsacties op grond van artikel 3 van richtlijn 2009/22 in te stellen, heeft bij de Oostenrijkse rechterlijke instanties een verbodsactie ingesteld tegen het gebruik van alle in deze algemene voorwaarden opgenomen bedingen alsmede een vordering tot publicatie van de te wijzen uitspraak. Hij legt hieraan ten grondslag dat deze bedingen alle in strijd zijn met wettelijke verboden en de goede handelspraktijken.

32. De rechter in eerste aanleg heeft alle vorderingen toegewezen met uitzondering van de vordering met betrekking tot beding 8 inzake de betaling van een toeslag in geval van koop op rekening. Deze rechter heeft, ervan uitgaand dat in beginsel de Rome-I-verordening van toepassing is, geoordeeld dat beding 12 inzake de keuze van het toepasselijke recht op grond van artikel 6, lid 2, van die verordening ongeldig is, aangezien de rechtskeuze niet tot gevolg mag hebben dat de consument de bescherming verliest die hij geniet op grond van de wetgeving

11. Het *Promusicae-arrest* (HvJ EG 29 januari 2008, C-275/06, ECLI:EU:C:2008:54) wordt gezien als de eerste zaak waar een dergelijke belangenafweging in relatie tot het internettijdperk werd aangegeven.
12. E. Kannekens & N.A.N.M. van Eijk, 'Oneerlijke handelspraktijken: alternatief voor privacyhandhaving', *Mediaforum* 2016, afl. 4, p. 102-109 (www.ivir.nl/publicaties/download/1800).