NJ 2017/392

Dommering, E.J.

Publication date
2017
Document Version
Final published version
Published in
Nederlandse Jurisprudentie

NJ 2017/392

HOF VAN JUSTITIE VAN DE EUROPESE UNIE
19 oktober 2016, nr. C-582/14
(M. Ilešič, A. Prechal, A. Rosas, C. Toader, E. Jarašiūnas)
m.nt. E.J. Dommering

Art. 2 onder a, 7 onder f Privacyrichtlijn 1995

RvdW 2016/1231
Module Privacy en persoonsgegevens 2016/1146
ECLI:EU:C:2016:779

Verzoek om een prejudiciële beslissing ingediend door het Bundesgerichtshof (hoogste federale rechter in burgerlijke en strafzaken, Duitsland) bij beslissing van 28 oktober 2014.

Verwerking van persoonsgegevens. Begrip, persoonsgegevens'. Internetprotocoladressen. Bewaring door een aanbieder van onlinemediadiensten. Nationale regeling volgens welke geen rekening kan worden gehouden met het gerechtvaardigde belang van de voor de verwerking verantwoordelijke persoon.

1. Art. 2 onder a Privacyrichtlijn 1995 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. Art. 7 onder f Privacyrichtlijn 1995 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.

Patrick Breyer tegen Bondsrepubliek Duitsland

Hof van Justitie EU:

Arrest

1 Het verzoek om een prejudiciële beslissing betreft de uitlegging van de artikelen 2, onder a), en 7, onder f), 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 (*PB* 1995, L 281, p. 31).

2 Dit verzoek is ingediend in het kader van een geding tussen P. Breyer en de Bondsrepubliek Duitsland over de registratie en bewaring door de Bondsrepubliek Duitsland van Breyers internetprotocoladres (hierna: 'IP-adres') bij zijn bezoek van verschillende websites van Duitse federale instellingen.

Toepasselijke bepalingen

Unierecht

3 Overweging 26 van richtlijn 95/46 luidt:
"Overwegende dat de beschermingsbeginselen moeten gelden voor elk gegeven betreffende een geïdentificeerde of identificeerbare persoon; dat, om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde persoon te identificeren; dat de beschermingsbeginselen niet van toepassing zijn op gegevens die op zodanige wijze anoniem zijn gemaakt dat de persoon waarop ze betrekking hebben niet meer identificeerbaar is; dat de gedragscodes in de zin van artikel 27 een nuttig instrument kunnen zijn om een indicatie te geven omtrent de middelen waarmee de gegevens anoniem kunnen worden gemaakt en kunnen worden bewaard in een vorm die identificatie van de betrokkene niet langer mogelijk maakt".

4 Artikel 1 van deze richtlijn luidt:
"1. De lidstaten waarborgen in verband met de verwerking van persoonsgegevens, overeenkomstig de bepalingen van deze richtlijn, de bescherming van de fundamentele rechten en vrijheden van natuurlijke personen, inzonderheid van het recht op persoonlijke levenssfeer.
2. De lidstaten mogen het vrije verkeer van persoonsgegevens tussen lidstaten beperken noch verbieden om redenen die met de uit hoofde van lid 1 gewaarborgde bescherming verband houden."

5 Artikel 2 van die richtlijn luidt:
"In deze richtlijn wordt verstaan onder:
a) 'persoonsgegevens', 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;

b) 'verwerking van persoonsgegevens', hierna 'verwerking' te noemen, elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;

[…]

d) 'voor de verwerking verantwoordelijke', de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam die, respectievelijk dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer het doel van en de middelen voor de verwerking worden vastgesteld bij nationale of communautaire wettelijke of bestuursrechtelijke bepalingen, kan in het nationale of communautaire recht worden bepaald wie de voor de verwerking verantwoordelijke is of volgens welke criteria deze wordt aangewezen;

[…]

f) 'derde', de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam, niet zijnde de betrokkene, noch de voor de verwerking verantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de voor de verwerking verantwoordelijke of de verwerker gemachtigd zijn om de gegevens te verwerken;

[…]"

6 Artikel 3 van richtlijn 95/46, met als opschrift 'Werkingssfeer', bepaalt:

"1. De bepalingen van deze richtlijn zijn van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

2. De bepalingen van deze richtlijn zijn niet van toepassing op de verwerking van persoonsgegevens:

— die met het oog op de uitoefening van niet binnen de werkingssfeer van het gemeenschapsrecht vallende activiteiten geschiedt zoals die bedoeld in de titels V en VI van het Verdrag betreffende de Europese Unie en in ieder geval verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de staat (waaronder de economie van de staat, wanneer deze verwerkingen in verband staan met vraagstukken van staatsveiligheid), en de activiteiten van de staat op strafrechtelijk gebied;

[…]"

7 Artikel 5 van deze richtlijn luidt:

"De lidstaten bepalen binnen de grenzen van de bepalingen van dit hoofdstuk nader de voorwaarden waaronder de verwerking van persoonsgegevens rechtmatig is."

8 Artikel 7 van richtlijn 95/46 luidt:

"De lidstaten bepalen dat de verwerking van persoonsgegevens slechts mag geschieden indien:

a) de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend, of

b) de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene, of

c) de verwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de voor de verwerking verantwoordelijke onderworpen is, of

d) de verwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene, of

e) de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of die deel uitmaakt van de uitoefening van het openbaar gezag die aan de voor de verwerking verantwoordelijke of de derde aan wie de gegevens worden verstrekt, […] is opgedragen, of

f) 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."

9 Artikel 13, lid 1, van richtlijn 95/46 bepaalt:

"De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in artikel 6, lid 1, artikel 10, artikel 11, lid 1, artikel 12 en artikel 21 bedoelde rechten en plichten indien dit noodzakelijk is ter vrijwaring van

[…]

d) het voorkomen, het onderzoeken, opsporen en vervolgen van strafbare feiten of schendingen van de beroepscodes voor gereglementeerde beroepen;

[…]"

Duits recht

10 § 12 van het Telemediengesetz (wet betreffende onlinemedia) van 26 februari 2007 (BGBl. 2007 I, p. 179; hierna: 'TMF') luidt:

"1. De aanbieder van diensten mag persoonsgegevens in verband met de terbeschikkingstelling van onlinemedia slechts verzame-

len en benutten voor zover deze wet of een ander wettelijk voorschrift dat expliciet op onlinemedia betrekking heeft, dit toestaat of de gebruiker zijn toestemming heeft gegeven.

2. De aanbieder van diensten mag persoonsgegevens die voor de terbeschikkingstelling van onlinemedia zijn verzameld, slechts voor andere doeleinden benutten, voor zover deze wet of een ander wettelijk voorschrift dat expliciet op onlinemedia betrekking heeft, dit toestaat of de gebruiker zijn toestemming heeft gegeven.

3. Tenzij iets anders is bepaald, zijn de voor de bescherming van persoonsgegevens geldende regels van toepassing, ook wanneer de gegevens niet automatisch worden verwerkt."

11 In § 15 TMG is bepaald:

"1. De aanbieder van diensten mag persoonsgegevens van een gebruiker slechts verzamelen en benutten voor zover dit noodzakelijk is om het gebruik van onlinemedia mogelijk te maken en te factureren (gebruiksgegevens). Als gebruiksgegevens worden in het bijzonder aangemerkt:

1) criteria met het oog op de identificatie van de gebruiker;

2) gegevens over begin en einde van het betrokken gebruik, alsook over de omvang ervan, en

3) gegevens over de onlinemedia die de gebruiker heeft gebruikt.

2. De aanbieder van diensten mag gebruiksgegevens van een gebruiker over het gebruik van verschillende onlinemedia samenvoegen, voor zover dit voor de facturering aan de gebruiker nodig is.

[…]

4. De aanbieder van diensten mag gebruiksgegevens na afloop van het gebruik benutten, voor zover zij voor de facturering aan de gebruiker nodig zijn (factuurgegevens). Om aan wettelijke, statutaire of contractuele bewaartermijnen te voldoen, mag de aanbieder van diensten de gegevens afschermen. […]"

12 Volgens § 3, lid 1, van het Bundesdatenschutzgesetz (federale wet betreffende gegevensbescherming) van 20 december 1990 (BGBl. 1990 I, p. 2954) zijn '[p]ersoonsgegevens […] specifieke gegevens over persoonlijke of zakelijke omstandigheden betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene). […]'

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.

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 be-

zoek 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, EU:C:2011:771, punt 51 (*NJ* 2012/479, m.nt. P.B. Hugenholtz; *red.*)), 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 exploitant — 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, 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, EU:C:2011:771 (*NJ* 2012/479, m. nt. P.B. Hugenholtz; *red.*)), 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 96/45 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 web-

site 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 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.

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, EU:C:2003:596, punt 43 (*NJ* 2004/248; *red.*), en 16 december 2008, *Satakunnan Markkinapörssi en Satamedia*, C-73/03, 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, 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, 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, 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.

Het Hof (Tweede kamer) verklaart voor recht: [zie *cursieve* kop].

Noot

1. In deze zaak worden twee belangrijke beslissingen gegeven over de uitleg van art. 2 onder a en art. 7 onder f Privacyrichtlijn 1995 (95/46/EG) die ook van belang blijven onder de nieuwe privacyverordening van 27 april 2016 (2016/679/EU) die in april volgend jaar van kracht wordt. Het gaat over de betekenis van het begrip 'persoonsgegeven' in art. 2 onder a en over de ruimte die lidstaten hebben om invulling te geven aan art. 7 onder f. Art. 7 onder f is de algemene uitzondering (de 'balancing provision') dat de verwerking van persoonsgegevens zonder toestemming van het datasubject is toegestaan in het gerechtvaardigde ('legitimate') belang van de verwerker of derden aan wie de data zijn ontsloten, tenzij zich daartegen de fundamentele rechten en vrijheden van het datasubject verzetten (in het Engels staat er: die belangen 'are overriden by' die rechten). In de verordening zijn dit respectievelijk art. 4 onder 1 en art. 6 lid 1 onder f.

2. De zaak begint in Duitsland waar de politieke activist Breyer bezwaar had gemaakt tegen het feit dat federale overheidsdiensten de IP-adressen van de bezoekers op hun sites registreren en bewaren zonder daarvoor toestemming van de gebruikers te vragen. De uitlegvraag ontstond, omdat de internetprovider van Breyer (zoals zovele providers) zogenaamde dynamische IP-adressen gebruikte. Het IP-adres is het nummer dat het adres vormt van de computer zodra deze op het internet is aangesloten. In de exacte definitie die de advocaat-generaal in deze zaak in paragraaf 1 van zijn conclusie geeft: 'Een internetprotocoladres (hierna: IP-adres) is een binaire numerieke reeks die, toegekend aan een apparaat (een computer, tablet of smartphone), dat apparaat identificeert en het mogelijk maakt om toegang tot het elektronische communicatienetwerk te krijgen. Om toegang tot internet te krijgen, moet het apparaat de numerieke reeks gebruiken die door de internetproviders is toegewezen.' Omdat er schaarste aan IP-nummers is, heeft een internetprovider minder nummers dan hij abonnees heeft. Per gebruik wordt er een nummer aan een gebruiker toegekend. Je kunt het vergelijken met een autoverhuurbedrijf dat vaste gebruikers van vast toegewezen huurauto's (internetverbinding) heeft, maar minder nummerborden dan auto's. Per gebruik wordt één van die nummerborden aan de toegewezen auto van de vaste gebruiker gehangen. De verhuurder (de internetprovider) weet wie er in de auto zit, maar derden zien alleen de auto met dat nummerbord rijden. Zo ook de federale overheden in Duitsland. Zij registreren en bewaren de nummers die hun site aandoen en dat zijn dus dikwijls dynamische IP-nummers, maar zij weten niet wie er achter dat tijdelijke nummer schuil gaat. Dat weet de internetprovider wel. Zowel de overheid als de internetproviders houden namelijk het verkeer op hun site bij en bewaren het om bij hackaanvallen te kunnen traceren wie toegang hebben gevraagd of op de site zijn geweest, zodat ze daders kunnen achterhalen en zich kunnen beveiligen. Toen Breyer op grond van de Duitse privacywetgeving bezwaar maakte tegen het registreren en vasthouden van zijn (dynamische) IP-nummer, rees dus de vraag of die wetgeving wel van toepassing was, meer precies: of een dynamisch IP-nummer wel een 'persoonsgegeven' is. De federale overheden die internetportalen exploiteren (zie conclusie van de advocaat-generaal nr. 23) zeiden van wel, omdat ze de identiteit van de gebruiker konden achterhalen bij de internetprovider van Breyer die de overheden immers dankzij het dynamische IP-nummer dat ze wel op hun site zagen, kenden. De vraag was dus of een identificerend gedragsgegeven (de handelingen van Breyer op de overheidssite die door het geregistreerde IP-nummer konden worden herleid tot het gedrag van één gebruiker afkomstig van één provider) door het opvragen en verkrijgen van aanvullende informatie bij de internetprovider *tot de persoon Breyer* konden worden herleid en daardoor toch een 'persoonsgegeven' kon worden. Vertaald naar de tekst van art. 2 onder a van de richtlijn is dat of Breyer een 'identificeerbaar' persoon was. En 'identificeerbaar' ben je volgens dat artikel ook als het '*indirect*' kan, dus kan worden afgeleid uit aanvullende gegevens buiten het gegeven sec. De Duitse appelrechter gaf Breyer gedeeltelijk gelijk: deze vond de dynamische IP-adressen persoonsgegevens, indien de gebruiker zelf aanvullende identificerende gegevens prijs gaf (bijvoorbeeld door zijn emailadres in te vullen bij toegang tot de website). Voor het overige werd het beroep verworpen. Het Bundesgerichtshof stelde de vraag in alle breedte bij het Hof van Justitie EU aan de orde.

3. Het HvJ EU had al beslist dat 'statische' IP-nummers (dus een aan een gebruiker toegekend uniek IP-nummer) persoonsgegevens zijn (de zaak *Scarlet*, C-70/10, HvJ EU 24 november 2011) en dat daarop de datarichtlijn van toepassing is. De vraag hoe het zit met het dynamische IP-adres lag echter nog open. De A-G had in zijn conclusie benadrukt dat de gestelde vraag beperkt was tot de verhouding websiteprovider-internetserviceprovider-abonnee van de serviceprovider (zijn conclusie onder 49-50). Voorts had hij zich afgevraagd of het om een objectief (wat kan de houder van het dynamische IP-adres in het algemeen?) of een subjectief (wat kan de houder van het dynamische IP-adres in het concrete geval?) criterium ging, een discussie die in de Duitse doctrine woedde. Het HvJ EU geeft op die controverse geen duidelijk antwoord, maar formuleert mijns inziens een op de situatie toegesneden geobjectiveerd criterium, in verschillende stappen. De richtlijn lijkt niet uit te sluiten dat niet alle informatie om het datasubject te identificeren bij de houder van het dynamische IP-adres berust. De mogelijkheid on die informatie te vergaren, moet een rechtmatig middel zijn (de aanvullende informatie bij de derde moet door deze rechtmatig vergaard en bewaard worden) en niet, slechts door een 'excessieve inspanning' (bijvoorbeeld door de vereiste tijd, te maken kosten en de benodigde mankracht) verkregen kunnen worden ('zodat het gevaar voor identificatie in werkelijkheid onbeduidend is'). De onderhavige situatie kan aan dit criterium voldoen, omdat de houder van het dynamische IP-adres zich kan wenden tot de Data Autoriteit om die aanvullende informatie bij de internetserviceprovider op te vragen (in de algemene bewoordingen van het Hof: 'voor de aanbieder van onlinemediadiensten juridische mogelijkheden 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.').

4. Om de rechtmatigheid van de verwerking en opslag bij de internetserviceprovider vast te stellen, kwam de tweede gestelde vraag in beeld: mocht deze de te individualiseren gebruiksgegevens van het datasubject opslaan? Volgens het Duitse recht mocht hij die gegevens alleen opslaan voor zakelijke doeleinden (verband houdend met de verschafte toegangsdienst: in casu facturering van het internetgebruik). De vraag was daarom of dit een toegestane implementatie van de 'balancing provision' van het algemeen geformuleerde art. 7 onder f van de richtlijn was. Met de A-G vindt het Hof dat dit niet een *concretisering* (vallende binnen de manoeuvreerruimte van een lidstaat) was maar een verboden *beperking* van de richtlijnbepaling was. Het verwijst daarvoor naar zijn eerdere beslissing in de zaak *ASNEF en FECEMD* (C-468/10 en C-469/10, HvJ EU 24 november 2011, r.o. 47-48).

5. De vraag is wat de werking naar de toekomst van deze beslissing is, met name als het gaat om wat tegenwoordig heet 'big data'. Daarmee wordt gedoeld op de ontwikkeling dat steeds meer gegevens over groepen individuen worden verzameld, die in combinatie met andere verzamelde gegevens vergaande voorspellingen omtrent het gedrag en de eigenschappen van leden van de groep mogelijk maken zonder dat deze tot concrete leden van de groep herleidbaar zijn. De vrees bestaat dat daarom de 'big data'-verwerking buiten het domein van de dataverordening zal vallen, omdat deze data nooit 'persoonsgegevens' worden. Het zou heel goed mogelijk zijn dat er toch een beschermingsniveau kan worden gevonden, doordat het begrip 'persoonsgegeven' niet meer is beperkt tot de kennis die één persoon of organisatie heeft. Het gaat er dus om dat de betrokkene een sleutelstukje uit de puzzel in handen heeft dat zonder excessieve inspanningen de weg kan wijzen naar een elders rechtmatig opgeslagen gegeven dat samen het herleidbare persoonsgegeven kan vormen. Naarmate de big data-technologie toeneemt, zou het steeds minder 'excessief' kunnen worden om ook meer ingewikkelde puzzels waar de stukjes van de puzzel over meer individuen of organisaties zijn verspreid op hun individuele plaats te doen vallen. Daarbij kan er op worden gewezen dat de definitie van het criterium 'indirect' bij persoonsgeven in de verordening is aangescherpt tot: 'indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.' De tijd zal het leren.

E.J. Dommering