*Prof. mr. dr. G-J. Zwenne**

Nog enkele opmerkingen over IP-adressen en persoonsgegevens, identificeerbaarheid en 'single out'

184

Trefwoorden:
ip-adres, identificeerbaarheid, persoonsgegeven

Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Over de uitleg van dit kernbegrip uit het privacy- of gegevensbeschermingsrecht is onenigheid. Enige jaren geleden is onze privacytoezichthouder, toen het ging over de kwalificatie van IP-adressen, zich op het standpunt gaan stellen dat er al sprake is van een persoonsgegeven als daarmee de éne persoon kan worden onderscheiden van de ándere, ook als onbekend is wie deze persoon is. De toezichthouder rekte daarmee de reikwijdte van het begrip, en dus ook zijn toezichtdomein, vergaand op. Van de aldus door hemzelf verruimde bevoegdheid maakte de toezichthouder de afgelopen jaren zo een tiental keren enthousiast gebruik. In deze bijdrage een commentaar daarop.

1 Inleiding

Op 4 september 2012 wees de Hoge Raad een arrest dat niet in dit tijdschrift is besproken, maar niettemin interessant kan zijn voor de lezers ervan. In het arrest ging het erom wat de strafrechter moet doen als de identiteit van de verdachte onbekend is, met als gevolg dat die verdachte alleen kan worden aangeduid door middel van een voor hem of haar uniek nummer.[1] In zijn conclusie bij het arrest zette A-G Knigge uiteen dat in een dergelijk geval er sprake is van een 'anonieme, d.w.z. ongeïdentificeerde verdachte'. Zo een anonieme verdachte moet alsnog worden geïdentificeerd. Dat kan de rechter, zo legt de A-G uit, op de volgende wijze doen:

'(…) door te vragen naar naam, voornamen, geboorteplaats, geboortedatum, gba-adres en feitelijk adres. Als er niettemin twijfel is over de identiteit van de verdachte is de rechter bevoegd nader onderzoek te laten doen omtrent de identiteit van de verdachte bestaande uit het afnemen van en vergelijken van vingerafdrukken en uit onderzoek van een identiteitsbewijs.'

We kunnen daaruit opmaken dat, in elk geval in het strafprocesrecht, een verdachte die alleen met een nummer kan worden aangeduid, níét is geïdentificeerd. Zo een anonieme verdachte moet alsnog worden geïdentificeerd. En dat kan aan de hand van de daartoe gebruikelijke gegevens en documenten.

Verrassend is dat niet. Ook voor wie niet heel bekend is met het strafprocesrecht zijn de overwegingen over het vaststellen van de identiteit van de verdachte zonder moeite te volgen, omdat ze goed aansluiten bij wat we ook in het dagelijks leven verstaan onder identificatie en identificeerbaarheid. Voor wie nog belangstelling heeft voor de ontwikkeling van het gegevensbeschermingsrecht, is het toch de moeite waard om daarbij iets langer stil te staan. Dit omdat onze privacytoezichthouder, het College bescherming persoonsgegevens (in het vervolg: CBP[2] of ook wel het College), zich enige jaren geleden op het standpunt is gaan stellen dat er al sprake kan zijn van geïdentificeerde natuurlijke persoon, als het mogelijk is om deze persoon te onderscheiden van andere personen, ook als verder niet bekend is wie deze persoon is.

Voor de toezichthouder is voldoende dat deze persoon kan worden aangeduid door middel van een voor hem of haar uniek nummer, zoals een IP-adres, een MAC-adres of een andere apparaat-identifier, zodat die persoon vervolgens anders kan worden behandeld dan anderen. In deze opvatting is voldoende dat iemand kan worden

* **Gerrit-Jan Zwenne is hoogleraar Recht en de informatiemaatschappij aan de Universiteit Leiden en advocaat te Den Haag.** **Hij dankt Berend van der Eijk, Ard Jan Dunnik en Joanne van Eenennaam voor hun nuttige commentaar op een eerdere versie van deze bijdrage.**

1 HR 4 september 2012, ECLI:NL:HR:2012:BX4153, *RvdW* 2012/1085, *NJB* 2012/1959, *NJ* 2012/507, *NBSTRAF* 2012/314, m.nt. T.J. Kelder.

2 Er is grote verwarring over het hoofdlettergebruik in de voor het College bescherming persoonsgegevens gebruikte afkorting: Cbp of CBP? Omdat zowel de definitie van art. 1 onder k Wbp als de aanduiding in art. 51 lid 1 Wbp uitgaat van een hoofdletter en twee kleine letters, komt het mij voor dat 'Cbp' de juiste spellingswijze is. Enige bevestiging daarvan vind ik in recente parlementaire geschiedenis, zoals *Kamerstukken II* 2014/15, 33662, 1-24 en *Kamerstukken II* 2014/15, 34195, 1-8. Het belang van deze kwestie is betrekkelijk, zeker na de toevoeging van een nieuw lid 4 aan art. 51 Wbp, dat bepaalt dat de toezichthouder in het maatschappelijk verkeer gaat worden aangeduid als Autoriteit persoonsgegevens (Ap), zie *Kamerstukken II* 2014/15, 33662, A, p. 4 en B, p. 7.

geïsoleerd van anderen (*singled out*).[3] De toezichthouder stelt aldus 'individualiseren' gelijk aan 'identificeren' en voelt zich daarin gesteund door de Artikel 29 Werkgroep, die in dezelfde periode kwam met een advies waarin deze uitleg van het persoonsgegevensbegrip werd geïntroduceerd.[4]

Deze uitleg betekende een vergaande oprekking of verruiming van de reikwijdte van het persoonsgegevensbegrip en is om deze reden niet onomstreden. In Nederland en elders, zoals in Duitsland en Frankrijk maar ook in Brussel, heeft dit geleid tot nogal wat discussie.[5] In deze bijdrage ga ik deze discussie niet volledig uiteenzetten. Ik ben bij eerdere gelegenheden daarop al ingegaan en verwijs de geïnteresseerde lezer graag daarnaar.[6] Op deze plaats wil ik alleen enkele aspecten ervan belichten. Ik bespreek op welke wijze, en om welke redenen, de toezichthouder, ervoor heeft gekozen uit te gaan van een opgerekt persoonsgegevensbegrip. Het gaat daarbij vooral over IP-adressen, omdat onze privacytoezichthouder nu eenmaal vooral daarover uitspraken heeft gedaan. Maar vanzelfsprekend gaat de discussie verder dan dat. In brede zin gaat deze discussie over de vraag over de reikwijdte van de gegevensbeschermingswetgeving en het toezichtdomein van privacytoezichthouders.

Ik begin bij het begin en bespreek kort een van de eerste zaken (de eerste?) waarin de privacytoezichthouder gebruik is gaan maken van het opgerekte persoonsgegevensbegrip (par. 2). Aansluitend ga ik in op enkele van de argumenten die door de toezichthouder werden gebruikt in daaropvolgende zaken (par. 3), waarna ik mij enkele opmerkingen veroorloof over wat nou eigenlijk het probleem is (par. 4) Ik sluit af met enkele opmerkingen over ontwikkelingen in de rechtspraak en het proces met betrekking tot de totstandkoming van de algemene verordening gegevensbescherming (par. 5).

2 Ruzie tussen GeenStijl en GeenCommentaar

Op de website van het CBP is met enige moeite nog een persbericht uit 2001 te vinden waarin de toezichthouder stelt dat een IP-adres kwalificeert als persoonsgegeven als de desbetreffende internetaanbieder systematisch de datum, het tijdstip en de duur van gebruik ervan heeft vastgelegd.[7] Alleen met deze extra gegevens, en alleen in combinatie met zijn abonneebestand, kan een internetaanbieder zonder onevenredige inspanning, de internetgebruikers identificeren die met behulp van het IP-adres gebruikmaken van zijn internetdiensten.[8] In het persbericht meldde de toezichthouder dan ook zonder voorbehoud:

'(…) een IP-nummer is niet altijd een persoonsgegeven.'

Van deze alleszins begrijpelijke opvatting over persoonsgegevens werd zes jaar later door de toezichthouder afstand genomen. Eerst in zijn Richtsnoeren over de publicatie van persoonsgegevens op internet[9] en vervolgens in een opmerkelijke handhavingsactie, waarin het College er ineens van uitging dat een IP-adres hoe dan ook kwalificeert als een persoonsgegeven, omdat wordt verondersteld dat daarmee een individuele internetgebruiker kan worden onderscheiden van andere. Voor het College maakte het daarbij niet uit dat onbekend is wie deze internetgebruiker is.

De handhavingsactie betrof een ruzie tussen twee blogs.[10] De blog GeenCommentaar[11] had er last van dat de gebruikers van GeenStijl voortdurend de op zijn platform gevoerde discussies verziekten.[12] Om daaraan wat te doen, bedacht GeenCommentaar een list. De blog publiceerde een steunbetuiging aan het anarchistische krakersblad *Bluf*, in de wetenschap dat GeenStijlers (of zoals zij zichzelf noemen 'reaguurders') daarop, op de voor hen kenmerkende wijze, zouden reageren. Toen dat inderdaad gebeurde, legde GeenCommentaar de IP-adressen vast van deze GeenStijlers. De aldus opgestelde lijst gebruikte GeenCommentaar vervolgens om voortaan de vervelende reacties van de GeenStijlers te weren. De vanuit deze IP-adressen geposte berichten werden geblokkeerd. Daarmee was het probleem van verziekte discussies vooralsnog even opgelost, althans zolang de GeenStijlers van dezelfde IP-adressen gebruik bleven maken.

---

3 Vgl. CBP Richtsnoeren, 'Publicatie van persoonsgegevens op het internet', 11 december 2007, p. 9. Zie ook CBP Definitieve bevindingen onderzoek 'Geen Stijl IP-checker', kenm. z2008-01174, 27 oktober 2008.

4 Artikel 29 Werkgroep, Advies 4/2007 over het begrip 'persoonsgegeven' (WP136), 20 juni 2007, p. 11.

5 Zie bijv. C. Alberdingk Thijm, 'Franse rechter hecht aan privacy P2P-gebruiker', 22 december 2006, via www.solv.nl (laatst geraadpleegd op: 8 juli 2015); S. Hansell, 'I.P. Adress: Partially Personal Information', *The New York Times* 24 februari 2008 via www.thenewyorktimes.com (laatst geraadpleegd op: 8 juli 2015); R. Heijna, 'Duitse prejudiciële vragen: IP-adres een persoonsgegeven?', 18 februari 2015, via www.solv.nl (laatst geraadpleegd op: 8 juli 2015).

6 G-J. Zwenne, 'Over persoonsgegevens en IP-adressen en de toekomst van privacywetgeving', in: L. Mommers e.a. (red.), *Het Binnenste Buiten* (liber amicorum Aernout H.J. Schmidt), Leiden: 2010, p. 321-342; G-J. Zwenne, 'Over IP-adressen en persoonsgegevens, en het verschil tussen individualiseren en identificeren', *IR* 2011, afl. 1, p. 4-9 en G-J. Zwenne, *De verwaterde privacywet* (oratie Leiden), 12 april 2013 – te vinden op www.zwenneblog.weblog.leidenuniv.nl of www.zwenne.nl.

7 CBP, 'Een IP adres is niet altijd een persoonsgegeven', 19 maart 2001, z2000-0340; zie www.cbpweb.nl zoekterm 'IP adres' (laatstelijk geraadpleegd op 22 juni 2015).

8 *Kamerstukken II* 1997/98, 25892, 3, p. 47-50.

9 Publicatie van persoonsgegevens op internet, CBP Richtsnoeren, december 2007, *Stcrt.* 2007, 240, p. 27, te vinden op www.cbpweb.nl met zoekterm: 'richtsnoeren internet' (laatstelijk geraadpleegd op 22 juni 2015).

10 Een weblog wordt door het CBP omschreven als 'een website waar met enige regelmaat nieuwe berichten worden gepubliceerd die omgekeerd chronologisch op de site verschijnen en in een archief doorzoekbaar blijven', zie CBP Rapport Definitieve Bevindingen inzake onderzoek 'Geen Stijl IP-checker op www.geencommentaar.nl, oktober 2008, p. 3 voetnoot 1 te vinden op www.cbpweb.nl met zoekterm: 'onderzoek geenstijl IP-checker' (laatstelijk geraadpleegd op 29 juni jl.).

11 GeenCommentaar omschrijft zichzelf als 'blog over communicatie in turbulente tijden'.

12 GeenStijl is, naar eigen zeggen, 'tendentieus, ongefundeerd en nodeloos kwetsend'.

Over deze 'IP-checker' ontving het College, zo blijkt uit de stukken, welgeteld één klacht, waarschijnlijk van een gefrustreerde GeenStijler. De klacht werd nog dezelfde dag in behandeling genomen. Er volgde een onderzoek dat anderhalve maand later zowaar leidde tot een officieel rapport van bevindingen. De conclusie ervan was dat GeenCommentaar door het verwerken van deze IP-adressen, enige bepalingen van de Wbp zou hebben overtreden, zijnde de bepalingen betreffende de informatieplicht (art. 33 Wbp) en die betreffende een zorgvuldige verwerking en het vereiste van een verwerkingsgrondslag (resp. art. 6 en 8 Wbp).

Het is de moeite waard dit rapport zoveel jaren later nog eens door te lezen. Het werkt op boeiende wijze toe naar de conclusies ervan. Het College stelt voorop dat 'geredelijkerwijs' kan worden aangenomen dat de heer X, die de blog GeenCommentaar heeft ontworpen en als contactpersoon daarvoor optreedt, heeft te gelden als 'de verantwoordelijke', aangezien hij 'tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt'.[13] Vervolgens beredeneert het College dat er inderdaad sprake is van de verwerking van persoonsgegevens, en wel omdat de IP-adressen door de internetaanbieder eenvoudig zouden zijn te herleiden tot een natuurlijk persoon, de afnemer van het internetabonnement.[14]

Er valt veel af te dingen op deze argumentatie. Het is natuurlijk merkwaardig dat de conclusie over wie verantwoordelijke is, voorafgaat aan de beoordeling of er überhaupt sprake is van de verwerking van persoonsgegevens. Maar dat is misschien een kwestie van stijl. Erger is dat in het rapport wordt uitgegaan van aannames en veronderstellingen die veel minder vanzelfsprekend zijn dan ze worden voorgesteld. Zo is het maar de vraag of het voor een internetaanbieder altijd zo eenvoudig is om een IP-adres te herleiden tot de afnemer van het internetabonnement. Verondersteld wordt kennelijk dat de internetaanbieder systematisch de datum, het tijdstip en de duur van gebruik ervan heeft vastgelegd, wat natuurlijk maar de vraag is.[15] Zelfs als dat zo zou zijn, dan nog is het de vraag of de afnemer van het internetabonnement zonder meer gelijk kan worden gesteld met degene die gebruikmaakte van dat IP-adres – dat lijkt in elk geval onmogelijk als het gaat om plekken waar veel verschillende gebruikers gebruikmaken van een gedeelde internetaansluiting, zoals op het werk of de universiteit, of bij gebruik van gratis wifi in de trein en bus, op een luchthaven, in een fastfoodrestaurant, enz.[16] En daarbij gaat het College er gemakshalve ook aan voorbij dat deze internetaanbieder niet kan worden gelijkgesteld met de aanbieder van de blog, die door het CBP wordt aangemerkt als verantwoordelijke. Als er al sprake zou zijn van persoonsgegevens dan toch alleen voor zover het gaat om de internetaanbieder, niet om de dienstenaanbieder, en dan alleen voor zover deze beschikt over de gegevens die hem in staat stellen om te achterhalen wie de abonnee of de gebruiker was die gebruikmaakte van dat IP-adres.

3 Wat daarna kwam: Google, TomTom, Vodafone, enz.

Al heel snel bleek het rapport over de IP-checker van GeenCommentaar niet op zichzelf te staan. In een tiental latere handhavingsonderzoeken zien we dat de toezichthouder vrijwel steeds dezelfde, vaak naar zichzelf verwijzende standaardargumentatie gebruikt om telkens weer te kunnen komen tot de vaststelling dat er sprake is van de verwerking van persoonsgegevens.[17] Het gaat dan om onderzoeken naar gegevensverwerkingen door Google, TomTom, Vodafone, Tele2, KPN, T-Mobile, TP Vision, nogmaals Google, YD, NPO en recent nog Ziggo.[18]

Interessant is dat in de latere rapporten aanvullende argumenten worden opgenomen. Zo wordt verwezen naar rechtspraak die, naar het oordeel van de toezichthouder, steun zou bieden voor zijn opgerekte uitleg van wat persoonsgegevens zijn. Als we die rechtspraak erbij pakken, blijkt echter al snel dat het College nogal kort door de bocht redeneert. Een voorbeeld biedt de verwij-

13 Zie art. 1 onder d Wbp.

14 CBP Rapport Definitieve Bevindingen inzake onderzoek 'Geen Stijl IP-checker op www.geencommentaar.nl, oktober 2008, p. 7.

15 Zie weer *Kamerstukken II* 1997/98, 25892, 3, p. 47-50.

16 In Nederland werd gratis wifi vanaf ca. 2010 beschikbaar in fastfoodrestaurants. Eerder kon er wel al gebruik worden gemaakt van gratis internet (via een vaste verbinding) in universiteiten, lounges van luchtvaarmaatschappijen en dergelijke.

17 Zie resp. CBP Rapport Definitieve Bevindingen inzake ambtshalve onderzoek Cbp naar de verwerking van geolocatiegegevens door TomTom, N.V., 20 december 2011, par. 4.2.1, p. 20-21; CBP Rapport Definitieve Bevindingen inzake onderzoek naar de analyse van gegevens over en uit het mobiele dataverkeer door KPN, B.V., 29 mei 2013, par. 3.3, p. 56; CBP Rapport Definitieve Bevindingen inzake onderzoek naar de analyse van gegevens over en uit het mobiele dataverkeer door Tele2 Nederland B.V., 29 mei 2013, par. 3.3, p. 36-45; CBP Rapport Definitieve Bevindingen inzake onderzoek naar de analyse van gegevens over en uit het mobiele dataverkeer door T-Mobile Netherlands B.V., 29 mei 2013, par. 3.3, p. 48-52; CBP Rapport Definitieve Bevindingen inzake onderzoek naar de analyse van gegevens over en uit het mobiele dataverkeer door Vodafone Libertel B.V., 29 mei 2013, par. 3.3, p. 52-58; CBP Rapport Definitieve Bevindingen inzake onderzoek naar de verwerking van persoonsgegevens met of door een Philips smart-tv door TP Vision Netherlands N.V., 1 juli 2013, par. 3.2, p. 55-56; CBP Rapport Definitieve Bevindingen inzake onderzoek CBP naar het combineren van persoonsgegevens door Google, 11 november 2013, par. 4.2, p. 44; CBP Definitieve Bevindingen Onderzoek naar de verwerking van persoonsgegevens door YD voor behavioural targeting, 27 maart 2014, par. 2.4, p. 15; CBP Rapport Definitieve Bevindingen inzake onderzoek Cbp naar de verwerking van persoonsgegevens met cookies door de publieke omroep (NPO), 8 juni 2014, par. 4.4, p. 31; CBP Rapport Definitieve Bevindingen inzake onderzoek Cbp naar de verwerking van persoonsgegevens door Snappet, 14 juli 2014, par. 4.3, p. 30; CBP Rapport Definitieve Bevindingen inzake onderzoek naar de verwerking van persoonsgegevens met betrekking tot of door het gebruik van interactieve digitale televisiediensten van Ziggo, 28 april 2015, par 4.1, p. 29-30. De auteur van deze bijdrage heeft in enkele van deze gevallen de onderzochte partijen bijgestaan in de procedures daarover.

18 Opvallend is dat in een weer een ander rapport juist afstand lijkt te worden genomen van het uitgangspunt dat een IP-adres per definitie als persoonsgegeven moet worden aangemerkt. Zie het Rapport Definitieve Bevindingen inzake het onderzoek naar de verwerking van persoonsgegevens door Snappet (kenm. z2013-00795), 14 juli 2014, p. 18.

zingen naar het *Scarlet/Sabam*-arrest van het Europees Hof van Justitie.[19] Daarin gaat de Europese rechter in op de invoering van een 'filtersysteem' dat het enerzijds mogelijk maakt om de berichten die worden verstuurd over het netwerk van een internetaanbieder systematisch te analyseren, en daarbij ook de IP-adressen vast te leggen van de gebruikers die illegale inhoud via dat netwerk versturen. Vervolgens komt het Hof met de volgende overweging:

'Aangezien die IP-adressen de precieze identificatie van die gebruikers mogelijk maken, vormen zij beschermde persoonsgegevens.'[20]

Wie zich beperkt tot deze overweging kan misschien komen tot de conclusie dat IP-adressen per definitie als persoonsgegevens moeten worden opgevat. Wie echter de moeite neemt om de desbetreffende overweging helemaal te lezen – en waarom ook eigenlijk niet meteen de rest van het arrest? – ziet dat die conclusie niet uit het arrest volgt. Er kan uit het arrest hooguit worden opgemaakt dat een IP-adres kwalificeert als persoonsgegeven, voor zover het de precieze identificatie van gebruikers mogelijk maakt. In het feitencomplex dat ten grondslag ligt aan het arrest was de internetaanbieder (Scarlet) in staat om, onder andere door middel van een systematische analyse, met het IP-adres de gebruikers te identificeren. In die context moesten deze adressen dus, voor zover het ging om die internetaanbieder, inderdaad als persoonsgegevens worden opgevat. In een andere context, waar die precieze identificatie niet mogelijk is, ligt dat uiteraard anders.

Een ander voorbeeld bieden de verwijzingen, in verschillende rapporten van het College, naar de conclusie van Jääskinen in het *Google Spain*-arrest van vorig jaar.[21] Over het persoonsgegevensbegrip merkt de A-G op dat een internetzoekmachine automatisch persoonsgegevens verzamelt die betrekking hebben op de gebruikers ervan, dat wil zeggen, op de personen die zoektermen invoeren in de zoekmachine:

'Deze automatisch overgebrachte gegevens kunnen bestaan uit hun IP-adres, gebruiksvoorkeuren (taal, enzovoort) en natuurlijk de zoektermen zelf, die in het geval van het zogenoemde "egosurfen" (een zoekactie waarbij een gebruiker zijn eigen naam invoert) snel de identiteit van een gebruiker onthullen. Van personen met een gebruikersaccount, die zichzelf daarmee hebben geregistreerd, belanden de persoonlijke gegevens zoals namen, e-mailadressen en telefoonnummers, vrijwel altijd in de handen van de aanbieder van de internetzoekmachine.'[22]

Het College maakt daaruit op dat IP-adressen zonder meer kwalificeren als persoonsgegevens,[23] maar ook hier is dat niet wat er in de conclusie wordt gezegd. De A-G zegt, niets meer en niets minder dan dat IP-adressen niet per definitie kwalificeren als persoonsgegevens, maar wel in combinatie met andere gegevens als zodanig kunnen worden aangemerkt. Er zal sprake zijn van persoonsgegevens als een gebruiker zelf zijn eigen naam of e-mailadres of telefoonnummer verstrekt. Omdat er bij gebruik van een zoekmachine niet kan worden uitgesloten dat dergelijke gegevens in combinatie met elkaar worden verwerkt, behoeft de A-G in zijn conclusie vervolgens niet al te lang stil te blijven staan bij de vraag of er in die specifieke context persoonsgegevens worden verwerkt.[24] Ook als we de door de wetgever beoogde brede reikwijdte van het begrip in aanmerking nemen, zegt hij daarmee nog niet dat een IP-adres hoe dan ook als persoonsgegeven moet worden aangemerkt.

Ook andere rechtspraak waarnaar in de rapporten worden verwezen blijkt, soms zelfs al bij een oppervlakkige beschouwing, weinig of geen steun te bieden voor de conclusies die daaraan door het College worden verbonden.[25]

4 Wat is het probleem?

Over de ruzie tussen GeenCommentaar en GeenStijl kunnen we onze schouders ophalen. Het is natuurlijk maar een mening, maar het komt mij nogal vergezocht voor om in de 'IP-checker' een schending van privacyrechten, of andere fundamentele rechten en vrijheden, te zien. Ik geloof niet dat de reaguurders veel hinder ervan hebben ondervonden. Ik zie geen beperking van de vrijheid van meningsuiting, laat staan een risico op stigmatisering of discriminatie. En als het om privacy gaat lijken juist deze reaguurders heel goed in staat voor zichzelf op te komen. In zoverre vind ik het opmerkelijk

19 HvJ EU 24 november 2011, C-70/10 (*Scarlet/Sabam*).
20 HvJ EU 24 november 2011, C-70/10 (*Scarlet/Sabam*), r.o. 51.
21 Conclusie van N. Jääskinen van 25 juni 2013 in C-131/12 (*Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González*).
22 Conclusie van N. Jääskinen van 25 juni 2013 in C-131/12 (*Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González*), punt 48.
23 CBP Rapport Definitieve Bevindingen inzake onderzoek naar de verwerking van persoonsgegevens door YD voor behavioural targeting, 27 maart 2014, par. 2.4, p. 15, voetnoot 30; CBP Rapport Definitieve Bevindingen inzake onderzoek naar de verwerking van persoonsgegevens met cookies door de publieke omroep (NPO), 12 juni 2014, par. 4.4, voetnoot 86; CBP Rapport Definitieve Bevindingen inzake onderzoek naar de verwerking van persoonsgegevens door Snappet 14 juli 2014, par. 4.3, p. 30 voetnoot 87; CBP Rapport Definitieve Bevindingen inzake onderzoek naar de verwerking van persoonsgegevens met betrekking tot of door het gebruik van interactieve digitale televisiediensten van Ziggo, 28 april 2015, par. 4.1, p. 29, voetnoot 94.
24 Conclusie van N. Jääskinen van 25 juni 2013 in C-131/12 (*Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González*), punt 71.
25 Zie bijv. de verwijzingen in de verschillende rapporten naar HvJ EG 6 november 2003, C-101/01 (*Bodil Lindqvist*).

dat het College juist in deze zaak ervoor heeft gekozen om zijn beperkte onderzoekscapaciteit in te zetten. Ik houd het er maar op dat er indertijd geen dringender zaken waren die de aandacht van de toezichthouder vroegen.[26]

Een vraag die dan gesteld kan worden is of er dan andere situaties zijn te bedenken waarin de verwerking van IP-adressen, of andere apparaat-identifiers, wél een onaanvaardbare inperking van de fundamentele rechten en vrijheden van de internetgebruiker zou kunnen betekenen, ook als de identiteit van die gebruikers niet bekend is. Het College en de Artikel 29 Werkgroep verwijzen daarvoor wel naar behavourial advertising en de uitgebreide en gedetailleerde profielen ('extensive profiles' en 'very detailed user profiles') die met behulp van cookies en IP-adressen van internetgebruikers kunnen worden opgesteld.[27] Echter, zoals de werkgroep zelf ook vaststelt in zijn advies daarover, kunnen dergelijke profielen waarschijnlijk zonder meer worden aangemerkt als persoonsgegevens, juist doordat ze uitgebreid en gedetailleerd zijn.[28] Om de risico's van het gebruik van dergelijke profielen te beperken is het daarom niet nodig om uit te gaan van het single-out-criterium of om op andere wijze het persoonsgegevensbegrip op te rekken.

Zijn er dan andere onaanvaardbare beperkingen van, of inbreuken op, privacy- of gegevensbeschermingsrechten die niet kunnen worden opgelost zonder het persoonsgegevensbegrip op te rekken? Er zou kunnen worden gedacht aan geo-blocking. Dat betreft de door omroepen en andere contentaanbieders (zoals NPO of Netflix) soms wel gebruikte methode om, meestal op basis van IP-adressen, te verhinderen dat we via internet in het buitenland kunt kijken naar een schaatswedstrijd of televisieserie, waarvan de uitzendrechten kennelijk zijn beperkt tot Nederland. Maar is dat voldoende reden om IP-adressen of andere apparaat-identifiers te brengen onder de reikwijdte van het persoonsgegevensbegrip? Het kan ergerlijk zijn, maar daarmee is het nog niet per se een inbreuk op een fundamenteel recht. En als dergelijk geo-blocking problematisch zou zijn, dan is het helemaal niet zo vanzelfsprekend dat dit moet worden opgelost door gegevensbeschermingswetgeving en de toezichthouders daarop. In haar plannen om te komen tot een digitale markt in de EU gaat de Europese Commissie in elk geval ervan uit dat mogelijke problemen met geoblocking langs andere wegen moeten worden opgelost.[29]

En wat als vergelijkbare IP-filters worden gebruikt om individuen uit te sluiten van andere, essentiële informatiebronnen? Wat als een IP-adres wordt gebruikt om prijsdiscriminatie toe te passen? Is het aanvaardbaar dat de ene collega, vanwege het door hem gebruikte IP-adres, voor zijn vliegticket een andere prijs moet betalen dan de andere? Het is voorstelbaar dat wetgever of toezichthouder daartegen optreedt. Maar ook dan is de vraag of het gegevensbeschermingsrecht de beste (meest effectieve, minst disproportionele) middelen biedt. Als het gaat om verboden prijsdiscriminatie, ligt het misschien meer voor de hand dat dit wordt beoordeeld aan de hand van de Wet gelijke behandeling. Of misschien aan de hand van het consumentenrecht, bijvoorbeeld de regels over oneerlijke handelspraktijken. En dat geval ligt in de rede dat dit wordt aangepakt door het College voor de Rechten van de Mens of de Autoriteit Consument en Markt.

Er zijn misschien andere zaken denkbaar waarin de verwerking van IP-adressen, of andere apparaat-identifiers, wél een onaanvaardbare beperking van fundamentele rechten zou kunnen betekenen. Echter, als we kijken naar de redenen die de privacytoezichthouder geeft zien we daarvan welbeschouwd maar weinig terug. In alle gevallen volstaat de toezichthouder met de algemene stellingname dat er sprake is van een privacyinbreuk, zonder te specificeren waaruit die bestaat, met daarbij telkens dezelfde doelredeneringen en verwijzingen naar eigen eerdere standpunten (zogenoemde Wc-eendargumentatie). Niet erg overtuigend allemaal.

5 Het laatste woord

Het laatste woord is aan de rechter. En het allerlaatste woord aan de wetgever. Zo gaat dat in een democratische rechtsstaat.

Wat betreft de rechter is de verwachting dat we op een termijn van één tot twee jaar antwoord krijgen op de vraag of een IP-adres, of een andere device-identifier, per definitie moet worden aangemerkt als persoonsgegeven, omdat een internetaanbieder in staat wordt geacht de gebruiker ervan te identificeren. Het Duitse Bundesgerichtshof heeft op 17 december vorig jaar het Hof van Justitie van de EU de prejudiciële vraag gesteld of, vrij vertaald, de definitie van het persoonsgegevensbegrip zo moet worden uitgelegd:

'(…) dat een internetprotocoladres, dat door een dienstenaanbieder in verband met de toegang tot zijn website wordt opgeslagen, voor deze aanbieder reeds dan een persoonsgegeven vormt, wanneer een derde (zijnde: de aanbieder van de internettoegang) beschikt over de bij-

26 Uit de indertijd gehanteerde Uitgangspunten en Beleidsregels Werkwijze CBP, *Stcrt*. 2004, 190, p. 11 blijkt dat de toezichthouder geen onderzoek instelt als er sprake is van (a) geringe en/of incidentele overtreding, (b) als voorzienbaar is dat een actie van het CBP geen resultaat zal opleveren of (c) als de behandeling van de klacht onevenredige inspanning van de toezichthouder zou vergen.

27 Artikel 29 Werkgroep, Opinion 2/2010 on online behavioural advertising (WP 171) 22 June 2010. CBP Rapport Definitieve Bevindingen inzake onderzoek naar de verwerking van persoonsgegevens door YD voor behavioural targeting, 27 maart 2014, p. 117, 128, 129; voetnoten 350, 418, 419 en 420(!).

28 Artikel 29 Werkgroep, Opinion 2/2010 on online behavioural advertising (WP 171) 22 June 2010, p. 3 en 4.

29 European Commission – Press release: Digital Single Market Strategy: European Commission agrees areas for action, Brussels, 25 March 2015, te vinden op http://europa.eu/rapid/press-release_IP-15-4653_en.htm (laatst geraadpleegd 22 juni 2015).

komende kennis die nodig is om de betrokken persoon te identificeren?'[30]

In deze zaak gaat het dus erom of een dienstenaanbieder, zoals iemand die een website of een blog als GeenCommentaar beschikbaar stelt, een persoonsgegeven verwerkt als hij IP-adressen vastlegt van voor hem niet te identificeren gebruikers. Daarbij wordt ervan uitgegaan dat een andere aanbieder, zijnde de internetaanbieder die aan deze gebruiker het IP-adres heeft verstrekt, met de hem beschikbare middelen in staat is deze gebruiker te identificeren. De door het Hof te beantwoorden vraag is dan of dit betekent dat het IP-adres alléén voor de internetaanbieder een persoonsgegeven is, of ook voor de dienstenaanbieder die zelf niet de gebruiker kan identificeren.

Voor wat de wetgever vindt van de discussie over het persoonsgegevensbegrip is van belang wat daarover is en wordt gezegd in het kader van de discussies over de privacy- en gegevensbeschermingswetgeving van de toekomst, de algemene verordening gegevensbescherming. Inmiddels hebben de Commissie, het Europees Parlement en de Raad hun oordeel daarover gegeven. Daaruit kan worden opgemaakt dat de Uniewetgever waarschijnlijk onverminderd blijft uitgaan van een persoonsgegevensbegrip waarbij identificeerbaarheid, en dus niet individualiseerbaarheid of single out – zoals het College voorstaat, het doorslaggevende criterium is.

In het voorstel van de Commissie uit januari 2012 werd het single-out-criterium überhaupt niet genoemd. Vervolgens hebben zowel de Artikel 29 Werkgroep als enkele leden van het Europees Parlement erop aangedrongen in de tekst van de verordening op te nemen dat single out voldoende zou zijn om te spreken van een persoonsgegeven.[31] In de versie die uiteindelijk door het Parlement is aangenomen komt het single-out-criterium daarentegen niet meer in die betekenis voor. In die tekst komt de term 'single out' nog in één overweging voor, maar alleen bij de uiteenzetting van de middelen waarmee een datasubject uiteindelijk kan worden geïdentificeerd. We kunnen daaruit opmaken dat de mogelijkheid om iemand van anderen te onderscheiden (single out) in combinatie met andere middelen wel kan bijdragen aan de identificeerbaarheid. Als zelfstandig criterium, dat op zichzelf zou kunnen leiden tot de kwalificatie als persoonsgegeven, heeft het in de thans voorliggende voorstellen echter geen betekenis meer.[32]

Uit de verslagen van de besprekingen van de Raad blijkt dat onze regering en die van andere lidstaten helemaal geen voorstander zijn van het oprekken van het persoonsgegevensbegrip met criteria als 'singling out'.[33] In de General Approach van de Raad van 15 juni 2015 komt de term dan ook niet meer voor.

Alles wat we nu over de verordening kunnen zeggen is speculatief zolang er geen overeenstemming is tussen Commissie, Parlement en Raad. Vooralsnog lijkt het niettemin onwaarschijnlijk dat we single out als zelfstandig criterium terugzien in de eindversie van de verordening. De discussie is daarmee waarschijnlijk afgesloten. Immers, als er al redenen zouden zijn om uit te gaan van een opgerekt persoonsgegevensbegrip, en daarmee van een vergaande uitbreiding van het toezichtdomein van de privacytoezichthouder, dan is de beslissing daarover aan de wetgever, niet aan die toezichthouder zelf.

---

30 Request for a preliminary ruling from the Bundesgerichtshof (Germany) lodged on 17 December 2014 – *Patrick Breyer/Bundesrepublik Deutschland* (Case C-582/14), te vinden op curia.europa.eu met zoekterm 'Breyer' of 'C-582/24'.

31 Zie het rapport van LIBE-rapporteur Jan Philips Albrecht: Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (COM(2012)0011 – C7-0025/2012, o.a. Amendments 25, 28 en 84, p. 16, 24 en 82. Artikel 29 Werkgroep, Opinie 1/2012 over de voorstellen voor hervorming van het gegevensbeschermingskader (WP191), 23 maart 2012; Artikel 29 Werkgroep, Advies 08/2012 met aanvullende input voor de besprekingen over de hervorming van de gegevensbeschermingswetgeving, 5 oktober 2012.

32 Recital. 23 luidt: 'The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person *to identify or single out* the individual directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous data, which is information that does not relate to an identified or identifiable natural person. (…)' (de cursivering heb ik toegevoegd).

33 In zijn Kamerbrief van 2 september 2013 zei de bewindspersoon het zo: 'Wat artikel 4 (begripsbepalingen) betreft, is er geen enkele steun voor het verder verfijnen van het begrip "persoonsgegevens" met categorieën als "singling out". De voorgestelde definitie lijkt Nederland en veel lidstaten al gecompliceerd genoeg.' Aldus *Kamerstukken II* 2012/13, 32761, 51, p. 2.