Regulering van IP-adressen (en andere mogelijke identifiers)

Zwenne, G.J.

Regulering van IP-adressen (en andere mogelijke identifiers)

G-J. Zwenne[*]

Inleiding

Zijn IP-adressen persoonsgegevens? Volgens de wetgever soms wel en soms niet. Het hangt er vanaf. Een IP-adres is een persoonsgegeven als daarmee, al dan niet in combinatie met andere gegevens, zonder onevenredige inspanning de identiteit van een natuurlijke persoon kan worden vastgesteld of achterhaald. In een eerdere bijdrage aan dit tijdschrift[1] heb ik uiteengezet dat privacytoezichthouders daarover anders zijn gaan denken. Inmiddels stellen zij zich op het standpunt dat IP-adressen[2] eigenlijk altijd als persoonsgegevens moeten worden aangemerkt of in elk geval als zodanig moeten worden behandeld. De toezichthouders brengen zo IP-adressen onder de werkingssfeer van de privacywet waarop zij toezicht houden. In het licht van wat kan met IP-adressen en de privacyimplicaties daarvan, is enig begrip op te brengen voor dit standpunt. En toch is dit onjuist, want in strijd met de privacywet en -richtlijn, en de uitgangspunten daarvan.[3]

In deze bijdrage, die het vervolg vormt van op voornoemde eerdere bijdrage, bespreek ik waarom het niet alleen onjuist is maar ook ongelukkig en ongewenst om het de reikwijdte van het persoonsgegevensbegrip zover op te rekken dat IP-adressen altijd daaronder vallen. Dat doet er evenwel niet aan af dat het gebruik van IP-adressen onze bewegingsvrijheid op internet kan beperken. In de afsluitende paragraaf doe ik daarom enkele suggesties voor regulering van IP-adressen.

Niet alles is een persoonsgegeven (of wel dan?)

De Wet bescherming persoonsgegevens (Wbp) en de Privacyrichtlijn 95/46/EG beogen een ruime bescherming te bieden tegen de risico's die verband houden met een ongebreidelde verzameling en verwerking van persoonsgegevens, en dat in een zeer veranderlijke context van snel opvolgende technologische ontwikkelingen. Om deze reden is de wetgever uitgegaan van een open persoonsgegevensbegrip dat wordt ingevuld aan de hand van objectieve en subjectieve criteria: gegevens worden aangemerkt als persoonsgegevens als, en voorzover, een verantwoordelijke, of iemand anders, in staat is om daarmee zonder onevenredige inspanning de identiteit van een individuele natuurlijke persoon vast te stellen of te achterhalen. Er wordt daarbij uitgegaan van alle middelen waarvan mag worden aangenomen dat die redelijkerwijs door de verantwoordelijke, of die ander, zijn in te zetten om die natuurlijke persoon te identificeren. Het uitgangspunt is dat van een redelijk toegeruste verantwoordelijke (objectief criterium). Ook wordt ook rekening worden gehouden met de bijzondere expertise of technische faciliteiten en dergelijke waarover de verantwoordelijke beschikt (subjectief criterium).[4]

De wetgeving is daarmee toekomstbestendig. De wet houdt rekening met ten tijde van het opstellen van de wet nog niet voorzienbare ontwikkelingen en toepassingen die met zich kunnen brengen dat individuen op enig moment aan de hand van bepaalde gegeven kunnen worden geïdentificeerd waar dat eerst misschien nog niet mogelijk was. Voorbeelden zijn sociale netwerken als Facebook. Daarmee is mogelijk geworden om zonder veel moeite, bijvoorbeeld aan de hand van de door anderen aangebrachte tags, te bepalen wie er allemaal zijn afgebeeld op de foto's van het feestje van een vage kennis waarop wij per ongeluk belandden. Voordat dit sociale netwerk beschikbaar was kon dat vaak niet, zodat het voor de meeste van ons niet mogelijk was om iemand met die foto's te identificeren.

Andere voorbeelden zijn de nog niet zo heel lang beschikbare gezichtsherkenningstoepassingen in digitale camera's[5] en thuiscomputers.[6] En uiteraard hebben ook verbeterde internetzoekmachines, indexeringsmogelijkheden, enz. het mogelijk gemaakt dat gewone gegevens, op zichzelf of in combinatie met andere gegevens, op een bepaald moment als persoonsgegevens moeten worden aangemerkt.

Omgekeerd kan ook. *Privacy-Enhancing-Technologies of PET-s*[7] beogen onder andere te waarborgen dat gegevens die eerst wel als persoonsgegevens werden aangemerkt, dat later niet meer zijn. PET-s ontdoen gegevens van die kenmerken die maken dat daarmee natuurlijke personen kunnen worden geïdentificeerd. Zo worden die gegevens buiten de werkingssfeer van de privacywet gebracht.

Soms ook proberen wetgevers en toezichthouders de mogelijkheden te beperken om gebruik te maken van gegevens waarmee natuurlijke personen kunnen worden geïdentifi-

---

* Gerrit-Jan Zwenne is, behalve redacteur van dit tijdschrift, advocaat bij Bird & Bird te Den Haag en universitair hoofddocent bij eLaw@Leiden, Centrum voor Recht in de Informatiemaatschappij, van de Universiteit Leiden.

1. G-J. Zwenne, 'Over IP-adressen en persoonsgegevens', *IR* 2011, 1, p. 4-9.
2. Onder verwijzing naar RFP760 (January 1980) wordt IP-adres wel omschreven als 'a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.'
3. Evenals in het dagelijks spraakgebruik wordt in de bijdrage de weinig specifieke term 'privacywet' gebezigd om de Wet bescherming persoonsgegevens (Wbp) aan te duiden.
4. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 48-49; Registratiekamer 27 maart 1995, 95.V.029.
5. Gezichtsherkenning is al enige tijd standaard beschikbaar op onder meer Canon IXUS en andere digitale camera's.
6. Het op iMac thuiscomputers standaard meegeleverde iPhoto kan na enige training zelfstandig bepalen wie op een foto staan, soms met verbazingwekkende resultaten.
7. In plaats van *PET-s* wordt tegenwoordig wel gesproken over '*privacy-by-design*'.

ceerd. Een voorbeeld betreft het invoering van het verbod op zgn. 'omgekeerd zoekdiensten', dat wil zeggen: de informatiediensten waarmee aan de hand van telefoonnummers kan worden gezocht naar de bijbehorende namen van abonnees.[8] Hoewel de telecom- en de privacytoezichthouders dit verbod niet wensen te handhaven[9] –onder andere omdat overtreding niet als privacyinbreuk zou worden opgevat– heeft deze wetswijziging wel ertoe geleid dat de belangrijkste internettelefoongidsen niet meer indexeerbaar zijn. Googlen op een vast of mobiel telefoonnummer leidt daardoor niet tot treffers in de goudengids.nl of detelefoongids.nl. Veel telefoonnummers zijn door deze, in de telecomwetgeving vastgelegde maatregelen dus voor velen van ons niet zonder onevenredige inspanning te herleiden tot geïdentificeerde natuurlijke personen. Soms wel, bijvoorbeeld als we het nummer herkennen of als het met de daarbijbehorende naam- en adresgegevens in onze telefoon is opgeslagen, of als we toegang hebben tot de abonneesystemen van telefoonmaatschappijen. Maar in veel gevallen toch niet.

Het persoonsgegeven is dus een open begrip, dat aan de hand van de feitelijke situatie moet worden ingevuld. Uitgaand van enerzijds de middelen waarover een redelijk toegerust verantwoordelijke beschikt en anderzijds bijzondere expertise of technische faciliteiten en dergelijke, moet iedere keer weer worden beoordeeld of er een concreet geval sprake van is of een natuurlijke persoon kan worden geïdentificeerd, of niet.

Een ISP die IP-adressen uitgeeft aan zijn abonnees moet daarom eerder worden geacht persoonsgegevens te verwerken dan degenen die niet weet aan wie welk specifieke IP-adres is uitgegeven. Maar zelfs dan nog moet er rekening mee worden gehouden dat deze ISP vaak niet weet, en niet kan weten, wie van dat IP-adres gebruik maken.[10] Als een interverbinding wordt gedeeld door meerdere gebruikers, zoals gebruikelijk in meerpersoonshuishoudens of in organisaties van enige omvang, kan ook de internetaanbieder niet achterhalen wie op een bepaald moment van een specifiek IP-adres gebruik maakte. Hetzelfde geldt voor de gebruikers die in een internetcafé of op een luchthaven of hamburgerrestaurant verbinding maken met internet via een gratis WiFi-verbinding. Ook dan is met behulp van het gebruikte IP-adres de identiteit van individuele gebruikers niet, of niet zonder onevenredige inspanningen, te achterhalen.[11]

Uitgaand van de door de wetgever geformuleerde criteria kunnen IP-adressen, en andere mogelijke identificatoren, dus soms wel maar zeker niet altijd als persoonsgegevens worden aangemerkt.

Aanpassing van de Privacywet?

Aan de hand van IP-adressen kunnen beslissingen worden genomen met betrekking tot geïndividualiseerde, maar niettemin nog niet geïdentificeerde of niet identificeerbare internetgebruikers. Dergelijke beslissingen kunnen vergaande implicaties hebben voor die internetgebruikers, bijvoorbeeld doordat hen toegang tot bepaalde informatie wordt ontzegd op basis van de geografische locatie die uit het IP-adres blijkt. Het is niet heel moeilijk in te zien dat daardoor onze bewegingsvrijheid op internet ernstig kan worden beperkt. En dat raakt aan verschillende fundamentele rechten, waaronder het recht op de bescherming van onze persoonlijke levenssfeer. Voor het CBP en andere toezichthouders lijkt dat de belangrijkste reden om IP-adressen als persoonsgegeven aan te merken of in elk geval als zodanig te behandelen, als daarmee nog niet de identiteit van de desbetreffende internetgebruikers is te achterhalen.[12]

Daarvoor is, zo heb ik aangegeven in mijn eerdere bijdrage,[13] enig begrip op te brengen. Er is in elk geval veel voor te zeggen om internetgebruikers in staat te stellen inzicht te hebben in, en zeggenschap te hebben over, wat er gebeurt met de door hen gebruikte IP-adressen, zeker als op basis daarvan belangrijke beslissingen over hen worden genomen. Echter, anders dan de toezichthouders stellen, bieden de wet en de richtlijn geen ruimte dit te doen door uit te gaan van een andere, verruimde uitleg van het persoonsgegevensbegrip. Voor de vraag of IP-adressen hebben te gelden als persoonsgegevens is bepalend of daarmee zonder onevenredige inspanning de identiteit van de desbetreffende internetgebruikers kan worden achterhaald, en niet wat de implicaties kunnen zijn van het gebruik ervan voor niet-geïdentificeerde individuele gebruikers.

Een interessante vraag is dan of de wet en richtlijn niet zouden moeten worden aangepast. In de wet en richtlijn zou kunnen worden opgenomen dat onder het begrip persoonsgegevens ook IP-adressen vallen, en wellicht ook andere daarmee vergelijkbare *identifiers*, zoals RFID-nummers of EIMI-codes. Een dergelijke aanpassing, die bij de aanstaande herziening van de richtlijn zou kunnen worden doorgevoerd, brengen met zich dat de regulering van IP-adressen op eenvormige wijze wordt ingebed in de bestaande, reeds voor persoonsgegevens geldende kaders. De verwerking van IP-adressen zou dan alleen nog mogelijk zijn als daarvoor goede en gerechtvaardigde redenen zijn, als dat niet onverenigbaar is met het doel waarvoor ze zijn verzameld, en alleen als de desbetreffende internetgebruikers daarover zijn geïnformeerd en desgewenst via kennisnemingsrechten daarover inzicht in kunnen hebben, enzovoorts. En dat allemaal onder toezicht van toezichthouders die zo nodig met de hen beschikbare handhavingsmiddelen de naleving van een en ander kunnen afdwingen.

---

8. De websites die nog steeds zgn. omgekeerdzoekdiensten aanbieden (zoals www.nummerzoeker.com) moeten worden geacht in strijd te zijn met het art. 11.6, derde lid, Tw. Dit is alleen anders als deze websites kunnen aantonen dat de daarin terug te vinden abonnees ermee hebben ingestemd dat hun gegevens via deze dienst kunnen worden teruggevonden - gelet op art. 3.2 van het Besluit universele dienstverlening en eindgebruikersbelangen is dat zeer onwaarschijnlijk.
9. OPTA Besluit van 17 oktober 2007, OPTA/IPB/2007/202118 (ooit gepubliceerd maar inmiddels niet meer terug te vinden op www.opta.nl) en CBP Besluit van 22 oktober 2007, z2007-00847 (niet gepubliceerd); zie ook *Stcrt*. 2007, 223.
10. P. Lundevall-Unger & T. Tranvik, 'IP-addresses – just a number?', *International Journal of law & Information Technology* 2011.
11. Zie G-J. Zwenne, 'Over IP-adressen en persoonsgegevens', *IR* 2011, 1, p. 4-9.
12. CBP Richtsnoeren, 'Publicatie van persoonsgegevens op het internet', 11 december 2007 *Stcrt*. 2007, 240; zie ook: CBP, 'GeenStijl IP-checker op GeenCommentaar' 27 oktober 2008 (z2008-01174); zie ook T. Wisman & M. van der Linden-Smith, 'My secret life as an average person', *IR* 2008, 4, p. 86-89.
13. G-J. Zwenne, 'Over IP-adressen en persoonsgegevens', *IR* 2011, 1, p. 4-9.

Op het eerste gezicht is deze benadering aantrekkelijk, omdat er niet heel veel voor nodig is om dit te realiseren. Aan de omschrijving van het begrip persoonsgegevens moeten een bijzinnetje worden toegevoegd waaruit blijkt dat daaronder ook IP-adressen vallen, en klaar is de wetgever. Als iets verder wordt gekeken en doorgedacht, blijkt echter al snel dat dit toch niet de meest geschikte of gelukkige benadering is. Ik bespreek puntsgewijs, niet noodzakelijk in volgorde van het grootste gewicht, enkele bezwaren daartegen:

Overkill. Een eerste bezwaar is dat op deze wijze veel meer wordt gereguleerd dan nodig is om internetgebruikers bescherming te bieden tegen de beslissingen die op basis van IP-adressen over hen kunnen worden genomen. Ook als in de wet staat dat IP-adressen altijd persoonsgegevens zijn, dan nog is duidelijk dat veel IP-adressen worden gebruikt in de context van *machine-to-machine* en *device-to-device connectivity*. In wat wel wordt aangeduid als het '*internet-of-things*' of '*ambient technology*' communiceren apparaten met elkaar, ook op basis van IP-adressen, zonder dat daarbij natuurlijke personen zijn betrokken. [14] In die context schiet regulering op basis van privacywetgeving (d.w.z. de Wbp en privacyrichtlijn 95/46/EG), zijn doel ver voorbij.[15]

Naleving en uitvoering. Op dit moment, uitgaande van een persoonsgegevensbegrip waaronder IP-adressen alleen vallen als daarmee een individu kan worden geïdentificeerd, is een veelgehoorde klacht dat de werkingssfeer van de privacywet onbegrensd is en de naleving ervan ingewikkeld of zelfs onmogelijk.[16] Een en ander wordt met het verruimen van het persoonsgegevensbegrip alleen maar erger – bijvoorbeeld waar het gaat om het inzagerecht, informatie- en meldingsplichten en de internationale doorgifte van de gegevens.[17]

Handhaving en toezicht. Ook waar het gaat om handhaving en toezicht is het verruimen van het persoonsgegevensbegrip niet zonder bezwaren, al was het maar omdat deze verruiming onvermijdelijk leidt tot onbeantwoordbare vragen over wie eigenlijk verantwoordelijke zijn met betrekking tot de verwerkingen die als gevolg daarvan onder het bereik van de privacywet komen te vallen. En, omdat dan ook onduidelijk is voor wie welke verplichtingen hebben te gelden, wordt handhaven dan lastig. Immers, het is vaste rechtspraak dat er alleen sancties mogen worden opgelegd met betrekking tot overtredingen van normen die voldoende voorzienbaar en duidelijk zijn[18].

Technologie(on)afhankelijkheid. De privacywet is niet zonder reden zoveel mogelijk technologieonafhankelijk geformuleerd, juist om de wet in een context van snelle technologische ontwikkelingen toekomstbestendig te maken en voorbereid te zijn op allerlei onvoorziene technieken en toepassingen. Het opnemen van het IP-adres in de begripsomschrijving van het begrip persoonsgegevens doet daaraan afbreuk, ook als er zou worden uitgegaan van meer algemene aanduidingen – zeg: het netwerkadres waarmee apparaten in een netwerk eenduidig geadresseerd worden binnen het TCP/IP-model.

Privacy-by-design. Een verruimde begripsomschrijving van het begrip persoonsgegevens haalt een streep door de ontwikkeling van '*privacy-by-design*' en *PET-s*, en alle inspanningen die daarvoor, niet in de laatste plaats door de toezichthouder, zijn gedaan.[19] Als IP-adressen per definitie als persoonsgegevens worden aangemerkt, heeft het weinig zin meer met behulp van technische en organisatorische maatregelen gegevensverwerkingen zo in te richten dat er geen sprake meer is van identificeerbaarheid. Althans, deze maatregelen leiden dan niet tot een vermindering van de nalevingskosten - een belangrijke reden is om daarin te investeren.

What's next? Als het er niet meer toedoet of de verantwoordelijke, of een ander, al dan niet beschikt over mogelijkheden om de identiteit van desbetreffende internetgebruiker, dan is de vraag welke andere gegevens ook nog als persoonsgegevens zouden moeten worden aangemerkt. En als iemand geacht wordt al te zijn geïdentificeerd als alleen het door hem of haar gebruikte IP-adres bekend is, moet alles dan niet alles wat een overigens onbekend individu kan aan-

14. Met de invoering van IPv6 is het totale aantal IP-adressen inmiddels voldoende is om ieder individueel atoom op de aarde een eigen unieke aanduiding te geven. Veel van die IP-adressen duiden geen natuurlijke personen aan.
15. Zie T.H.A. Wisman & A.R. Lodder, 'Hoeveel ruimte is er voor privacy op het internet van dingen', *IR* 2010, 6, p. 178 t/m 183.
16. Vgl. G-J. Zwenne et al, *Eerste fase evaluatie Wet bescherming persoonsgegevens. Literatuuronderzoek en knelpuntenanalyse*, Den Haag 2007, p. 12, 61, 64-68, 96, 137, 157 en 168; zie ook bijv. R.J.M. van der Horst, 'De Wet bescherming persoonsgegevens, gevolgen voor de organisatie en de automatisering', in J.E.J. Prins & J.M.A. Berkvens (red.), *Privacyregulering in theorie en praktijk*, Deventer 2002, 113; P. de Hert & S. Gutwirth, 'Veiligheid en grondrechten. Het belang van een evenwichtige privacypolitiek', in E.R. Muller (red.), *Veiligheid. Studies over inhoud, organisatie en maatregelen*, Alphen aan den Rijn 2004, p. 587-631; G-J. Zwenne et al, *Eerste fase evaluatie Wet bescherming persoonsgegevens. Literatuuronderzoek en knelpuntenanalyse*, Den Haag 2007, p. 12, 61, 64-68, 96, 137, 157 en 168.
17. Vgl A. Bloemen-Patberg, G-J. Zwenne & T. de Weerd, 'Wie bepaalt wat gebeurt met IP-adressen en verkeers- en locatiegegevens?' in E. Visser & M. Weij (red.), *Who controls the internet*, NVvIR Den Haag 2009, p. 90-91.
18. Interessant is dat ook de Art. 29 Werkgroep dit uitgangspunt uitdrukkelijk onderschrijft in zijn Opinion 10/2001 on the need for a balanced approach in the fight against terrorism <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp53en.pdf>; zie daarover: E Tikk, 'IP Addresses Subject to Personal Data Regulation' […]; zie verder o.a. EHRM 25 mei 1993, ECRM Series A, Vol. 260.
19. De website van het CBP noemt o.a.: R. Koorn et al, *Privacy Enhancing Technologies: Witboek voor beslissers*, Ministerie van Binnenlandse Zaken en Koninkrijkrelaties 2004; G.W. van Blarkom, J.J. Borking & J.G.E. Olk (eds.), *Handbook of Privacy and Privacy-Enhancing Technologies: The case of Intelligent Software Agents*, Den Haag 2003; S. Kenny & J.J. Borking, 'The Value of Privacy Engineering', *Journal of Information, Law and Technology* 2002/1; J. Borking & C. Raab, 'Laws, PETs and Other Technologies for Privacy Protection', *Journal of Information, Law and Technology* 2001/1.

duiden, worden aangemerkt als persoonsgegeven? Wat is dan geen persoonsgegeven meer?
Er zijn nog nog wel meer redenen te noemen waarom het bepaald ongelukkig is om het wettelijk persoonsgegevensbegrip zover te verruimen dat daaronder ook altijd IP-adressen, en wellicht nog andere *identifiers*, komen te vallen.[20] Alles bij elkaar is onwenselijk om op deze wijze te proberen regels te stellen met betrekking tot het gebruik van IP-adressen. Daarmee is evenwel niet gezegd dat alles maar moet mogen met IP-adressen als daarmee geen individuen zijn te identificeren.

Waarborgen voor gebruik IP-adressen

Ook als onze identiteit niet kan worden achterhaald kan het heel vervelend of zelf bedreigend zijn als wij op basis van gedetailleerde persoonsprofielen worden lastig gevallen met banner-advertenties die, onder andere door het gebruik van IP-adressen, verbazend nauw aansluiten bij de mogelijk zorgvuldig door ons verborgen gehouden persoonlijke voorkeuren. Als we ons al over dergelijke vormen van *behavorial advertizing*[21] heen kunnen zetten, dan nog is daarmee niet gezegd dat al het gebruik van IP-adressen aanvaardbaar is. Wat als individuele, ongeïdentificeerde internetgebruikers op grond van IP-adressen worden geweerd van een internetdiscussieforum?[22] Wat te denken van auteursrechtorganisaties die op basis van de door hen als 'verdacht' aangemerkte IP-adressen de internetverbindingen van individuele, maar ongeïdentificeerde uploaders (of misschien zelfs downloaders) laten afsluiten?[23] En wat als autoriteiten systematisch gaan bijhouden van welke IP-adressen gebruik wordt gemaakt door al te kritische, subversieve bloggers of twitteraars? Andere, ernstigere gevallen laten zich denken.
In deze gevallen komen fundamentele rechten, zoals het recht op privacy maar ook de vrijheid van meningsuiting, onder druk te staan. En dat, in alle gevallen, zonder dat er sprake is van identificeerbaarheid en derhalve evenmin van bescherming op grond van de privacywet. In deze gevallen kan er aanleiding zijn om op de een of andere manier beperkingen te stellen aan het gebruik van IP-adressen.
Hoe dan? De te stellen beperkingen zijn vanzelfsprekend afhankelijk van het soort van risico's waartegen internetgebruikers zouden moeten worden beschermd. Enigszins voor de vuist weg, want een echte analyse daarvan heb ik in het kader van deze bijdrage niet gedaan, ligt voor de hand om in elk geval te voorzien in waarborgen tegen gebruik van IP-adressen voor andere doeleinden dan waarvoor deze zijn bedoeld te worden gebruikt, zijnde het aanduiden van de locatie van apparaten in een netwerk ten behoeve van de communicatie tussen die apparaten. In het verlengde daarvan ligt in de rede om te voorzien in waarborgen tegen het individualiseren van internetgebruikers, alsmede toch ook waarborgen gericht op het voorkomen dat IP-adressen op enig moment kunnen gaan worden gebruikt om internetgebruikers alsnog te identificeren.
Een voor de hand liggend beginpunt zou zijn de ISP die aan zijn gebruikers IP-adressen uitgeeft. Voorstelbaar is dat de ISP als standaardfaciliteit aan internetgebruikers de mogelijkheden biedt om gebruik te maken op internet zonder dat zij aan de hand van het gebruikte IP-adres gemakkelijk kunnen worden geïndividualiseerd.Zo een faciliteit zou door de ISP aan gebruikers kunnen worden aangeboden, min-of-meer op dezelfde wijze als de bij mobiele telefoondiensten aangeboden faciliteit waarmee de nummerherkenning kan worden uitgezet. Deze, in de wet gewaarborgde faciliteit[24] stelt ons in staat om desgewenst te bellen zonder dat bekend is welk nummer wij gebruiken. Een zelfde soort faciliteit zouden IPS's kunnen aanbieden als het gaat om het gebruik van internet, oftewel: een faciliteit die ons in staat stelt gebruik te maken van internet zonder dat ons IP-adres bekend wordt gemaakt, althans zonder dat wij aan de hand van dat IP-adres eenvoudig kunnen worden geïndividualiseerd. Natuurlijk. Wie dat wil kan nu al gebruik maken van *anonymizers*[25] en vergelijkbare internetdiensten waarmee email en ander internetverkeer wordt geschoond van de informatie waaruit iets blijkt over de herkomst ervan. Echter, behalve dat de betrouwbaarheid van dergelijke diensten niet altijd evident is, zijn dergelijke faciliteiten voor de meeste gebruikers niet echt toegankelijk of gebruiksvriendelijk genoeg. Een gebruiksvriendelijke faciliteit, waarmee bijvoorbeeld mogelijk wordt om gebruik te maken van vaak wisselende IP-adressen, maakt het onmogelijk of tenminste heel veel moeilijker om internetgebruikers te individualiseren en op basis daarvan hun bewegingsvrijheid te beperken.
Voor het aanbieden van dit soort of andere faciliteiten is niet per sé regelgeving nodig. Een ISP kan daartoe, binnen de geldende wettelijke kaders,[26] zelf overgaan. Een ISP-brancheverenigingzou kunnen overgaan tot het formuleren van *best practises* of het opstellen van zelfregulering.

20. Vgl. G-J. Zwenne, 'Over persoonsgegevens en IP-adressen, en de toekomst van privacywetgeving', in L. Mommers et al (red.), *Het binnenste buiten* 2010, p. 335-337.
21. J. Koeter, 'Behavioral targeting en privacy: een juridische verkenning van internetgedragsmarketing', *IR* 2009, 4, p. 104-111.
22. 'GeenStijl IP-checker op GeenCommentaar' 27 oktober 2008 (z2008-01174).
23. Zo is naar verluid wel gebeurd dat een heel studentenhuis werd afgesloten omdat er één gebruiker iets had gedaan wat volgens de ISP en/of anderen niet door de beugel kon.
24. Art. 11.9, eerste lid, onder a, Tw; daarover Zwenne 2009, *T&C Telecomrecht*, art. 11.9, aant. 1-2.
25. Zie bijvoorbeeld www.squidoo.com/hideipaddress en < http://proxify.com>.
26. Vgl. de verwijderings- of anonimiseringsverplichtingen van art. 11.5 Tw en de bewaarplicht van art. 13.2a Tw.