Over persoonsgegevens en IP-adressen, en de toekomst van privacywetgeving

Gerrit-Jan Zwenne■[1]

Aanleiding

Ik tik de tekst van deze bijdrage in op een netbook-computer die via een draadloze verbinding van KLM Air France is verbonden met internet. Het IP-adres waarvan ik gebruik maak is 194.209.131.192. Is dit nummer een persoonsgegeven? Is het mogelijk dat ik, of misschien iemand anders, aan de hand van dit 12-cijferig nummer, al dan niet in combinatie met andere beschikbare gegevens, kan worden geïdentificeerd? Ik denk van niet. Op dit moment zijn er schat ik ongeveer 75 reizigers in deze lounge en ongeveer de helft daarvan lijkt gebruik te maken van de internetverbinding. De dienst is gratis. Of eigenlijk: inbegrepen in de prijs van het vliegticket. Voor het gebruik van de dienst heb ik geen identificerende gegevens opgegeven. Weliswaar hebben alle bezoekers van deze lounge zich bij binnenkomst bekendgemaakt door middel van instapkaart en paspoort, maar daarmee valt voorzover ik kan overzien niet te achterhalen wie van hen precies gebruik maakt van de internetverbinding.

In deze context is het, denk ik, niet vanzelfsprekend dat het IP-adres een persoonsgegeven betreft. Voorbijgaand aan de onwaarschijnlijke situatie dat KLM Air France iedere zitplaats in de lounge zou hebben voorzien van verborgen videocamera's met gezichtsherkenningsfaciliteiten of andere meer geavanceerde surveillance-technologie, lijkt het uitgesloten dat iemand aan de hand van dit specifieke gegeven direct of indirect kan worden geïdentificeerd. Ik ga er dus vanuit dat het van KLM Air France of wie dan ook een onevenredige inspanning zou vragen om aan de hand van dit IP-adres te achterhalen wat de identiteit is van de internetgebruikers in de lounge.

Niet iedereen is het met mij eens. In de discussie over de werkingssfeer van privacywetgeving zijn privacytoezichthouders de afgelopen jaren steeds verdergaande (om niet te zeggen: radicalere) standpunten gaan innemen. Van het nog redelijk genuanceerde standpunt dat het er maar vanaf hangt of IP-adressen kunnen worden aangemerkt als persoonsgegeven is men uitgekomen op het standpunt dat deze specifieke gegevens eigenlijk altijd

---

■ Gerrit-Jan Zwenne is universitair hoofddocent bij eLaw@Leiden, Centrum voor Recht in de Informatiemaatschappij, en partner bij Bird & Bird Advocaten in Den Haag.

moeten worden aangemerkt als persoonsgegevens, of in elk geval zo moeten worden behandeld. Dit omdat deze gegevens, in combinatie met andere, door derden te verstrekken gegevens op enig moment het mogelijk zouden kunnen maken dat een natuurlijke persoon kan worden geïdentificeerd. De achterliggende redenering lijkt te zijn dat er, gelet op het belang van privacybescherming, beter te veel dan te weinig onder de werkingssfeer van de privacywet kan worden gebracht.

Er is, zeker naarmate 'instruments of mass surveillance' een alomtegenwoordig karakter beginnen krijgen,[2] begrip op te brengen voor deze redenering. En toch schiet deze om meerdere redenen haar doel voorbij. Als IP-adressen, en waarom niet nog andere identifiers, per definitie worden aangemerkt als 'persoonsgegevens' verliest dit begrip zijn onderscheidend vermogen. En dat kan uiteindelijk alleen maar leiden tot verdergaande afkalving van de privacywet.

In deze bijdrage bespreek ik de ontwikkeling van de opvattingen van privacytoezichthouders over IP-adressen en persoonsgegevens[3] en speculeer ik over hun, tot dusver nog niet erg duidelijk gemaakte beweegredenen. Zoals gezegd meen ik dat het bepaald onverstandig is het persoonsgegevensbegrip zo extensief te interpreteren. Omdat ik niettemin wel aanleiding zie om ten minste serieus na te denken over het stellen van beperkingen aan wat kan en mag met IP-adressen, doe ik een voorstel dat voortbouwt op bestaande regels in de telecomwetgeving.

Persoonsgegevens in de privacyrichtlijn en -wet

Er is sprake van een persoonsgegeven als het gaat om een gegeven waarmee direct of indirect een natuurlijke persoon kan worden geïdentificeerd. Aldus blijkt uit artikel 2, onder a, van privacyrichtlijn 95/46/EG, dat het begrip 'persoonsgegevens' definieert als:

> "iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon"

In dezelfde bepaling wordt aangegeven wat wordt verstaan onder identificeerbaarheid:

> "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"

2 Vgl. Klitou 2008.

3 In de bespreking van de ontwikkeling van de opvattingen van de Artikel 29 Werkgroep en CBP wordt voortgebouwd op de uiteenzetting in Bloemen-Patberg, Zwenne & De Weerd 2009.

In de preambule bij de richtlijn wordt aangegeven op welke wijze moet worden vastgesteld of iemand kan worden geïdentificeerd. Er moet, zo blijkt uit overweging 26, worden gekeken naar het volgende:

> "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;"

Uit dezelfde overweging blijkt dat er echter geen sprake is van persoonsgegevens als het gaat om:

> "[…] gegevens die op zodanige wijze anoniem zijn gemaakt dat de persoon waarop ze betrekking hebben niet meer identificeerbaar is."

De Wet bescherming persoonsgegevens (Wbp) heeft minder woorden nodig om hetzelfde te zeggen. Artikel 1, onder a, van de wet stelt dat onder een persoonsgegeven wordt verstaan:

> "elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon."

In de parlementaire geschiedenis[4] wordt ingegaan op het identificeerbaarheidscriterium. In vrijwel dezelfde bewoordingen als van de zo even genoemde overweging 26 van de richtlijn wordt aangegeven dat moet worden uitgegaan van alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door de verantwoordelijke dan wel enig ander persoon zijn in te zetten om die persoon te identificeren. Het uitgangspunt is dat van 'een redelijk toegeruste verantwoordelijke'. Onder verwijzing naar eerdere uitingen van de privacytoezichthouder[5] wordt opgemerkt dat er:

> "[i]n concrete gevallen rekening [moet] worden gehouden met bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke. Het gaat dus enerzijds om objectivering naar een redelijk toegeruste verantwoordelijke en anderzijds om subjectivering naar bijzondere expertise […]. Een onderzoeksinstituut als het CBS zal bijvoorbeeld gelet op zijn expertise, contacten en technische outillage, eerder in staat zijn gegevens te identificeren dan een individuele onderzoeker. Deze omstandigheid dient in de beoordeling of sprake is van een persoonsgegeven te worden meegewogen."

Voor de vraag of een IP-adres heeft te gelden als persoonsgegeven, en als zodanig onder de werking van de wet valt, is bepalend in hoeverre het mogelijk is om aan de hand van dit adres een natuurlijke persoon te identificeren. Het gaat erom in hoeverre degene die over dit gegeven beschikt in staat is daarmee de identiteit van een bepaalde natuurlijke persoon te weten

4 *Kamerstukken II* 1997-98, 25 892, nr. 3, bldz. 48-49.
5 Vgl. Registratiekamer 27 maart 1995, (kenm. 95.V.029).

te komen. En daarbij gaat het niet om de zuiver theoretische of hypothetische maar reële mogelijkheid dat de verantwoordelijke of iemand anders aan de hand van het IP-adres en met de hem redelijkerwijs beschikbare middelen ('expertise', 'contacten', 'technische outillage', enz.) in staat is deze identiteit te achterhalen.

In de parlementaire geschiedenis wordt, in de alinea na op de zo even aangehaalde alinea, ook ingegaan op de mogelijkheid dat bepaalde gegevens in verschillende contexten verschillende betekenissen kunnen hebben.

> "Wat blijkens het voorgaande voor de verantwoordelijke geldt, geldt bij het verstrekken van gegevens aan een derde uiteraard ook voor de ontvanger. Dat betekent dat de verantwoordelijke zich in een dergelijk geval zal moeten afvragen of de bewuste gegevens in handen van de ontvanger al dan niet als identificeerbaar zullen moeten worden aangemerkt. Bepalend is wat in de gegeven situatie redelijkerwijs mag worden verwacht. Naarmate een verstrekker over meer mogelijkheden beschikt om de risico's van identificatie door de ontvanger te voorzien of te beperken, mag van hem in dit opzicht meer zorgvuldigheid worden verwacht."

Het is goed mogelijk dat een bepaald gegeven ten opzichte van de éne persoon wel als persoonsgegeven kan worden aangemerkt en tegelijkertijd tegenover de ander niet. Een verantwoordelijke die beschikt over gegevens waarmee alleen hij in staat is natuurlijke personen te identificeren, kan deze gegevens verstrekken aan iemand anders. En als die andere dan niet in staat is daarmee de desbetreffende natuurlijke personen te identificeren, hebben deze gegevens tegenover die andere niet te gelden als persoonsgegevens. Het criterium is wat 'in de gegeven situatie redelijkerwijs mag worden verwacht.'

De Artikel-29-werkgroep over IP-adressen

Het overlegorgaan van nationale privacytoezichthouders, de Artikel 29 Werkgroep, stelt het onder meer tot zijn taak om de begrippen van de privacyrichtlijn 95/46/EG te verduidelijken.[6] De afgelopen jaren heeft de werkgroep zich verschillende keren uitgelaten over IP-adressen. Uit de desbetreffende werkdocumenten en opinies blijkt dat de opvattingen van de werkgroep zich hebben ontwikkeld. Eerst waren de standpunten nog redelijke genuanceerd en lieten ruimte voor de mogelijkheid dat deze gegevens niet altijd onder het bereik van de richtlijn vallen. Inmiddels is dat veranderd. In zijn latere opinies gaat de werkgroep ervan uit dat IP-adressen eigenlijk altijd en per

6 Oftewel "[d]oor uitwisseling van ervaringen tussen de nationale autoriteiten zal de Groep een coherente strategie voor de toepassing van de in de richtlijn neergelegde algemene beginselen aanmoedigen", aldus Art. 29 WG, Eerste jaarverslag, WP3, 25 juni 1997, bldz. 4. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1997/wp3_nl.pdf.

definitie moeten worden aangemerkt als persoonsgegevens, of in elk geval altijd als zodanig moeten worden behandeld.

Een van de eerste opmerkingen van de werkgroep over de kwalificatie van IP-adressen in termen van persoonsgegevens is te vinden in een eind vorige eeuw opgesteld verkennend werkdocument over verwerkingen van persoonsgegevens op internet.[7] De werkgroep merkt erin op dat 'bepaalde internetprotocol-adressen' persoonsgegevens kunnen zijn:

> "Het gebruik van infrastructuur is vaak rechtstreeks gebaseerd op de verwerking van persoonsgegevens, zoals bepaalde Internetprotocoladressen."

Volgens dit werkdocument moeten dus niet altijd alle IP-adressen per se worden aangemerkt als persoonsgegevens zijn, maar als het gaat om 'bepaalde' IP-adressen vaak wel.

Ongeveer een jaar later werkt de werkgroep dit verder uit. In zijn werkdocument over internet, privacy en online-gegevensbescherming[8] komt de werkgroep tot de conclusie dat in elk geval de door een ISP uitgegeven IP-adressen voor deze ISP als persoonsgegevens hebben te gelden. Dit omdat (of misschien: voorzover) kan worden aangenomen dat deze internetaanbieder systematisch de datum, het tijdstip, de duur en het aan hun gebruikers verstrekte (dynamische) IP-adres vastlegt. Volgens de werkgroep brengt dit met zich mee dat:

> "internetaanbieders en beheerders van lokale netwerken zonder veel moeite internetgebruikers [unnen] identificeren aan wie ze IP-adressen hebben verstrekt, doordat ze als regel systematisch de datum, het tijdstip, de duur en het verstrekte dynamische IP-adres van gebruikers in een logbestand vastleggen. Hetzelfde geldt voor internetdienstverleners die een logboek op de HTTP-server bijhouden. In deze gevallen is het buiten kijf dat men kan spreken van persoonsgegevens in de zin van artikel 2, onder a, van de richtlijn."

De werkgroep tekent daarbij wel aan dat dit voor andere internetpartijen wellicht anders is, omdat zij niet vanzelfsprekend in staat zijn om met het IP-adres internetgebruikers te identificeren. Daarbij maakt de werkgroep onderscheid tussen vaste IP-adressen waarmee identificatie geacht wordt eenvoudiger te zijn, en dynamische IP-adressen waarbij dat moeilijker is:

> "Anders is het als derden wel het dynamische IP-adres van een gebruiker kunnen achterhalen, maar dat niet kunnen koppelen aan andere gegevens die identificatie van de betrokken gebruiker mogelijk maken. Identificatie van internetgebruikers die een statisch IP-adres toepassen, is uiteraard eenvoudiger."

---

7 Art. 29 WG, Processing of Personal Data on the Internet, 23 februari 1999 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp16nl.pdf.

8 Art. 29 WG, Privacy on the Internet. An integrated EU Approach to On-line Data Protection, 21 november 2000 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37nl.pdf.

Daar voegt de werkgroep echter aan toe dat het toch vaak mogelijk zal zijn om degene die van het IP-adres gebruik maakt te identificeren, en wel door het vaste of dynamische IP-adres te koppelen aan andere gegevens die over de gebruiker zijn verkregen, bijvoorbeeld via cookies of datamining. Om deze redenen gaat de werkgroep ervan uit dat veel, maar toch niet per sé alle IP-adressen moeten worden aangemerkt als persoonsgegevens:

> "In veel gevallen is het echter wel degelijk mogelijk het IP-adres van gebruikers zodanig te koppelen aan andere (al dan niet openbaar beschikbare) persoonsgegevens dat deze gebruikers kunnen worden geïdentificeerd, vooral als gebruik wordt gemaakt van onzichtbare verwerkingsmethoden om aanvullende informatie over de gebruiker te verwerven (bijvoorbeeld met behulp van cookies die een unieke identificatiecode bevatten) of van moderne datamining gekoppeld aan grote databases met individueel identificeerbare gegevens over internetgebruikers."

Maar de werkgroep blijft redelijk genuanceerd en geeft nadrukkelijk aan dat niet is uitgesloten dat IP-adressen in voorkomende gevallen niet, althans niet voor iedereen, zijn aan te merken als persoonsgegevens, die vallen onder de werkingssfeer van de richtlijn:

> "Om deze reden wordt er, ook al is het wellicht niet in alle gevallen en niet voor alle internetpartijen mogelijk een gebruiker aan de hand van de op internet verwerkte gegevens te identificeren, in dit document van uitgegaan dat de mogelijkheid daartoe in veel gevallen wel degelijk bestaat en dat grote hoeveelheden persoonsgegevens waarvoor de richtlijnen op het gebied van persoonsgegevens gelden, op internet worden verwerkt."

Ook hier wordt derhalve aangegeven dat IP-adressen in veel gevallen moeten als persoonsgegevens moeten worden aangemerkt als persoonsgegeven. Maar niet altijd en evenmin ten opzichte van iedereen.

Deze nog steeds genuanceerde benadering werkt de werkgroep uit in een opinie over het begrip persoonsgegevens.[9] Waar het gaat om de identificeerbaarheid gaat de werkgroep uiteraard uit van de maatstaf uit overweging 26 van de preambule bij de richtlijn: er moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs zijn in te zetten door de verantwoordelijke of iemand anders. De werkgroep leidt daaruit af dat de theoretische of hypothetische mogelijkheid om een natuurlijke persoon te identificeren onvoldoende is om die persoon als identificeerbaar te beschouwen. Om te bepalen of sprake is van 'redelijkerwijs in te zetten middelen' moet rekening worden gehouden met alle relevante omstandigheden van het geval.

Als voorbeeld noemt de werkgroep de situatie dat een auteursrechthebbende de IP-adressenvan abonnees verzamelt waarvan wordt vermoed dat die inbreuk maken op zijn auteursrechten. Er is dan sprake van persoonsge-

9 Art. 29 WG, Opinion nr. 4/2007 on the concept of personal data, 20 november 2007 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_nl.pdf.

gevens als wordt aangenomen dat de rechthebbende via gerechtelijke procedures de beschikking kan verkrijgen over desbetreffende abonneegegevens:

> "Vooral in die gevallen dat het IP-adres wordt verwerkt met het doel de gebruikers van de computer te identificeren (bijvoorbeeld door de houder van een auteursrecht die computergebruikers wil aanklagen wegens schending van intellectuele-eigendomsrechten), gaat de voor de verwerking verantwoordelijke ervan uit dat de "redelijkerwijs in te zetten middelen" voor de identificatie van de betrokkenen beschikbaar zullen zijn, bijvoorbeeld via de rechtbanken waarop een beroep wordt gedaan, anders zou het verzamelen van de informatie geen zin hebben. Deze informatie moet dan ook als persoonsgegeven worden beschouwd."

Maar ook dan zijn er volgens de werkgroep nog veel voorbeelden waarbij identificatie met een IP-adres onmogelijk is, zoals het geval van een internetcafé waarbij gebruiker zich niet behoeft te identificeren:

> "In sommige gevallen is het voor bepaalde IP-adressen om diverse technische en organisatorische redenen niet mogelijk de gebruiker te identificeren. Een voorbeeld zijn de IP-adressen die zijn toegewezen aan computers in een internetcafé waar van de klanten geen legitimatie wordt verlangd. Hier zou kunnen worden aangevoerd dat de gegevens over het gebruik van computer X gedurende een bepaalde periode geen identificatie van de gebruiker met redelijkerwijs in te zetten middelen mogelijk maken en dat die gegevens daarom geen persoonsgegevens zijn."

Omdat niet in alle gevallen bekend is of er sprake is van identificeerbaarheid doet de werkgroep wel de aanbeveling dat internetdienstverleners voor de zekerheid alle IP-adressen als persoonsgegevens behandelen. Dit echter niet zozeer omdat het per definitie persoonsgegevens betreft, maar om praktische redenen:

> "De internetdienstverlener zal echter naar alle waarschijnlijkheid niet weten of het IP-adres in kwestie identificatie mogelijk maakt, en zal de aan dat IP-adres gekoppelde gegevens op dezelfde wijze behandelen als informatie die gekoppeld is aan IP-adressen van geregistreerde en identificeerbare gebruikers."

De ommekeer doet zich iets minder dan een half jaar later voor. In een opinie over internetzoekdiensten[10] neemt de werkgroep afstand van zijn tot dan toe consequent gevolgde standpunt betreffende IP-adressen moeten worden aangemerkt als persoonsgegevens. Zonder echt aan te geven waarom gaat de werkgroep in deze opinie ineens voorbij aan de nuancering dat moet worden gekeken naar de middelen waarover een bepaalde verantwoordelijke de beschikking heeft. Ook ziet de werkgroep geen ruimte meer voor de situatie waarin de éne gegevensverwerker wél identificatiemogelijkheden

10 Art. 29 WG, Opinion 1/2008 on data protection issues related to search engines, 4 april 2008 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf.

heeft en de andere niet, zodat IP-adressen voor de eerste wel persoonsgegevens betreffen maar voor de laatste niet:

> "Though IP addresses in most cases are not directly identifiable by search engines, identification can be achieved by a third party. Internet access providers hold IP address data. Law enforcement and national security authorities can gain access to these data and in some Member States private parties have gained access also through civil litigation. Thus, in most cases – including cases with dynamic IP address allocation – the necessary data will be available to identify the user(s) of the IP address."

De werkgroep meent dat een IP-adres hoe dan ook een persoonsgegeven betreft omdat identificatie door derden mogelijk kan zijn ('identification […] by a third party'). Weliswaar kan in de regel alléén de ISP achterhalen welke natuurlijke persoon van een IP-adres gebruik heeft gemaakt. Maar omdat 'bepaalde autoriteiten' en in voorkomende gevallen zelfs private partijen in staat zijn om van de ISP de nodige identificerende abonneegegevens te verkrijgen, meent de werkgroep dat er hoe dan ook sprake is van persoonsgegevens.

In lijn met deze opvatting, waarin de beschikbaarheid van de redelijkerwijs in te zetten identificatiemiddelen als het ware wordt verondersteld, zijn de voorwaarden die de werkgroep introduceert waar het gaat om het anonimiseren van gegevens:

> "Anonymisation of data should exclude any possibility of individuals to be identified, even by combining anonymised information held by the search engine company with information held by another stakeholder (for instance, an internet service provider). Currently, some search engine providers truncate IPv4 addresses by removing the final octet, thus in effect retaining information about the user's ISP or subnet, but not directly identifying the individual. The activity could then originate from any of 254 IP addresses. This may not always be enough to guarantee anonymisation."

Er kan volgens de werkgroep alleen dan worden gesproken van anonimisering of on-identificeerbaarheid als iedere mogelijkheid van identificering is uitgesloten ('exclude any possibility of individuals to be identified'). In de eerder gehanteerde, genuanceerdere benadering had nog kunnen worden gesteld dat gegevens zijn geanonimiseerd voorzover deze gegevens niet door iemand met de redelijkerwijs hem ter beschikking staande middelen kunnen worden gebruikt om een natuurlijke persoon te identificeren. Maar voor dergelijke nuanceringen ziet de werkgroep geen ruimte meer.

Daarmee is de werkgroep dus uitgekomen op het standpunt dat IP-adressen inmiddels, ook voor de internetpartijen die deze níet aan individuele gebruikers kunnen koppelen, altijd moeten worden aangemerkt als persoonsgegeven en als zodanig onder het bereik van de richtlijn vallen. En waar de werkgroep eerst niet uitsloot dat er in de context van bijvoorbeeld een internetcafé of een openbare bibliotheek geen sprake is identificeerbaarheid, gaat hij er in deze opinie vanuit dat er altijd zonder meer sprake is van persoonsgegevens.

Het CBP over IP-adressen

De opvattingen van het CBP over IP-adressen hebben eenzelfde ontwikkeling doorgemaakt als die van de werkgroep – niet helemaal onverwacht omdat het CBP een actief deelnemer is aan de werkgroep.

In het verleden lieten ook het CBP en zijn voorganger de Registratiekamer zich genuanceerd uit over IP-adressen en persoonsgegevens. Op de website van de toezichthouder zijn voorbeelden daarvan te vinden. Zo is er een brief uit 2001[11] waarin de Registratiekamer uiteenzet onder welke omstandigheden kan worden aangenomen wanneer met een IP-adres zonder onevenredige inspanningen de identiteit van een natuurlijke persoon kan worden vastgesteld. De toezichthouder parafraseert de parlementaire geschiedenis die weer voortbouwt op zijn eerdere correspondentie over hetzelfde onderwerp:[12]

> "Bij 'identified or identifiable' speelt vooral de vraag of de identiteit van de persoon redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Dit hangt mede af van de mogelijkheden waarover de houder beschikt en de bekendheid of beschikbaarheid van aanvullende informatie. Hierbij moet uitgegaan worden van een redelijk toegeruste houder. In concrete gevallen moet echter wel rekening worden gehouden met bijzondere expertise, technische faciliteiten en dergelijke van de houder. Het gaat dus enerzijds om objectivering naar een redelijk toegeruste houder en anderzijds om subjectivering naar bijzondere expertise."

Een en ander toepassend op IP-adressen komt de toezichthouder vervolgens tot het oordeel dat de door een ISP uitgegeven vaste of statische IP-adressen 'zonder meer' door deze ISP zijn te herleiden tot natuurlijke personen en dus als persoonsgegevens moeten worden aangemerkt. Voor dynamische IP-adressen is dit niet anders, tenminste als de ISP heeft vastgelegd op welk moment het adres door welke gebruiker werd gebruikt. Als de ISP dit evenwel niet heeft vastgelegd, kan er niet worden gesproken van persoonsgegevens. En hoewel de brief daarover niet erg duidelijk is, lijkt het uitgangspunt te zijn dat er niet kan worden gesproken van persoonsgegevens ten opzichte van anderen dan de ISP's, als deze anderen niet beschikken over de middelen om de internetgebruikers te identificeren.

---

11 CBP, 'Een IP adres is niet altijd een persoonsgegeven', 19 maart 2001, z2000-0340 www.cbpweb.nl/downloads_uit/z2000-0340.pdf.

12 Vgl. de parl. gesch, genoemd in voetnoot 5 en de brief van de Registratiekamer genoemd in voetnoot 4.

In verschillende publicaties over zgn. 'privacy enhancing technologies' gaat het CBP verder in op dit laatste aspect van het identificeerbaarheidscriterium, dat wil zeggen: de vraag in hoeverre er kan worden aangenomen dat er ten opzichte van de éne gegevensverwerker (zeg: de ISP) wél sprake kan zijn van persoonsgegevens en tegelijkertijd ten opzichte van anderen niet. Zonder daarbij in te gaan op IP-adressen zet de toezichthouder in dit kader uiteen dat er géén sprake is van identificeerbaarheid, en dus niet van persoonsgegevens, als voor het identificeren de medewerking van derden is vereist en deze medewerking niet kan worden afgedwongen.[13] Een gegeven is alleen een persoonsgegeven voor degenen die in staat zijn met dit gegeven een natuurlijke persoon te identificeren, en niet voor degenen die dat niet kunnen:

> "niet-identificeerbaarheid [wordt] aangenomen als hiervoor de medewerking van derden buiten de macht en zeggenschap van de verantwoordelijke noodzakelijk is"

In de regel worden IP-adressen daarom ten opzichte van ISP's aangemerkt als persoonsgegevens. Er kan maar hoeft niet per sé ten opzichte van anderen sprake zijn van persoonsgegevens, maar alleen voorzover deze anderen door de ISP's (of eventueel anderen) in staat worden gesteld daarmee een natuurlijke persoon te identificeren.[14]

De publicatie van de zo-even besproken opinie van de werkgroep over zoekdiensten brengt ook voor het CBP de ommekeer. In zijn persbericht over de opinie meldt de toezichthouder zonder enig voorbehoud dat nu eindelijk:

> "ondubbelzinnig [wordt] vastgesteld dat IP-adressen persoonsgegevens vormen."[15]

---

13 CBP 2002.

14 Idem Van Esch 2008, p. 75-76; Van Esch & Blok 2007, p. 206.

15 CBP-persbericht Internetzoekmachines moeten privacy respecteren, 7 april 2008 (www.cbpweb.nl/docum–enten/pb_20080407_internetzoekmachines.shtml); naar aanleiding van twee uitspraken van Cour d'appel de Paris 13ème chambre, section B Arrêt du 27 avril 2007 en section A Arrêt du 15 mai 2007 kwam de Franse privacytoezichthouder met het volgende verontwaardigde persbericht: "In two successive rulings issued in April and May 2007, the Court of Appeal of Paris judged that IP addresses collected during searches and findings of internet counterfeiting acts do not enable, even indirectly, any identification of physical persons, and that consequently they do not constitute personal data. Concerned about the consequences of such an analysis of Internet privacy protection, CNIL contacted the Minister of Justice and the Public Prosecutor to the Cour de Cassation (Supreme Court) in an attempt to lodge an appeal against both rulings in the interest of the law. In a letter dated 8 October 2007, the Minister of Justice agreed to lodge the appeal to the Cour de Cassation who should issue its ruling sometime in 2008. It should be noted that, in an opinion published on 20 June 2007, the data protection authorities of EU Member States issued a reminder that IP addresses were indeed to be regarded as personal data." (http://www.cnil.fr/english/main-issues/tracking-web-surfers/); zie daarover Peter Fleischer in zijn blogbericht van 15 februari 2008 (http://peterfleischer.blogspot.com).

Natuurlijk, deze wellicht wat overenthousiaste uiting betreft een persbericht en niets meer dan dat. En er kon indertijd wellicht nog worden volgehouden dat de persvoorlichter de opinie van de werkgroep wat kort-door-de-bocht had samengevat, en dat de toezichthouder het niet zo had bedoeld. Iets meer dan een half jaar later blijkt echter dat het CBP wel degelijk afstand heeft willen nemen van zijn eerdere, meer genuanceerde opvatting over IP-adressen. In zijn richtsnoeren[16] voor de publicatie van persoonsgegevens op het internet stelt de toezichthouder zich op het standpunt dat het niet meer uitmaakt dat ISP's de gegevens in feite niet gebruiken om natuurlijke personen te identificeren. Voldoende is dat er daartoe een mogelijkheid bestaat, bij de ISP zelf of bij anderen.

Ook lijkt de toezichthouder afstand te willen nemen van de genuanceerdere opvatting dat sommige gegevens voor de éne gegevensverwerker wel als persoonsgegevens moeten worden aangemerkt (omdat deze gegevens hem in staat stellen natuurlijke personen te identificeren), terwijl diezelfde gegevens tegelijkertijd voor anderen niet als zodanig hebben te gelden (als die anderen niet in staat zijn daarmee iemand te identificeren). Als eenmaal is vastgesteld dat een IP-adres in de context van een ISP een persoonsgegeven betreft – en daarvan wordt per definitie uitgegaan – dan werkt dat volgens de richtsnoeren dus door in al het verdere gebruik van het gegeven: ergens eens een persoonsgegeven betekent derhalve altijd en overal een persoonsgegeven. De richtsnoeren stellen:

> "Een IP-adres is een persoonsgegeven omdat het door een derde – de internetaanbieder – eenvoudig te herleiden valt tot een natuurlijk persoon, de afnemer van het internetabonnement. Dit geldt ook voor dynamische IP-adressen die worden verwerkt in combinatie met datum en tijd. Het maakt geen verschil dat een verantwoordelijke het IP-adres niet zal gebruiken om een persoon mee te identificeren. Het feit dat de mogelijkheid bestaat bij de verantwoordelijke of bij een derde om dit te doen, is voldoende."

Wel onderkennen de richtsnoeren dat 'in sommige gevallen' met behulp van IP-adressen alleen rechtspersonen worden geïdentificeerd. Maar dat doet er niet aan af dat er 'in de meeste gevallen' toch wel sprake zal zijn van persoonsgegevens en er 'dus' alle gegevens hoe dan ook als zodanig moeten worden behandeld.

> "Dat het IP-adres in sommige gevallen naar een rechtspersoon leidt, in plaats van naar een natuurlijk persoon, doet niet af aan het feit dat het in de meeste gevallen wel degelijk om persoonsgegevens gaat en dat dus de hele verzameling moet worden behandeld conform de uitgangspunten van de Wbp."

16 CBP Richtsnoeren, 'Publicatie van persoonsgegevens op het internet', 11 december 2007 *Stcrt.* 2007, 240 www.cbpweb.nl/downloads_rs/rs_20071211_persoonsgegevens_op_internet_definitief.pdf.

Het is onduidelijk is wat er precies wordt bedoeld met deze opmerking. Voorzover er bedoeld is te zeggen dat gegevens over rechtspersonen in de meeste gevallen toch persoonsgegevens zijn, lijkt dat overduidelijk op gespannen voet te staan met de werkelijkheid. Er kan ook zijn bedoeld dat het in deze gevallen praktisch onmogelijk is om onderscheid te maken tussen de IP-adresssen die wél en niet kunnen worden gebruikt om natuurlijke personen te identificeren. Er is dan dus niet zozeer een verplichting om ook IP-adressen van rechtspersonen te behandelen alsof het persoonsgegevens zijn, maar veeleer een (gemakshalve veronderstelde) praktische onvermijdelijkheid.[17]

Een voor de hand liggende vraag is dan waarom er in deze gevallen geen technische of organisatorische maatregelen zouden kunnen worden genomen om de persoonsgegevens te scheiden van andere gegevens. In dezelfde lijn ligt de vraag waarom er geen privacy enhancing technologies zou kunnen worden toegepast om identificeerbaarheid te voorkomen. Het lijkt erop dat de toezichthouder geen vertrouwen meer heeft in dergelijke oplossingen. Dat zou opmerkelijk zijn, omdat nou juist de toezichthouder in het verleden (terecht) veel heeft geïnvesteerd in het ontwikkelen en doordenken van dergelijke PET's.[18]

Commentaar

De geschetste ontwikkeling van de opvattingen van de werkgroep en het CBP lenen zich voor een nadere beschouwing, zij het dat deze noodgedwongen een speculatief karakter heeft omdat er door hen maar weinig is losgelaten over hun beweegredenen.

Het lijkt aannemelijk dat deze beweegredenen allereerst liggen in het intelligenter worden van de technieken waarmee gegevens met elkaar in verband worden gebracht en internetgebruikers worden geïndividualiseerd. Indertijd, zo rond de eeuwwisseling, waren de mogelijkheden daartoe nog betrekkelijk beperkt. Inmiddels zijn zoek- en selectietechnologieën – denk aan: behavourial targeting, profiling, data mining, deep packet sniffing etc. – veel intelligenter geworden en daarbij breed beschikbaar, wat aanleiding kan zijn om veel eerder uit te gaan van identificeerbaarheid.

---

17 In een recent onderzoek volstaat het CBP grotendeels met verwijzingen naar de eigen richtsnoeren. Op het verweer dat niet alle IP-adres naar individuen verwijzen, reageert het CBP met de opmerking dat het dit argument 'niet steekhoudend' acht, omdat "het niet afdoet aan de herleidbaarheid tot een individu van een groot deel van de IP-adressen". Ofte wel: omdat een groot deel van de IP-adressen herleidbaar is tot individuen zijn alle IP-adressen persoonsgegevens. Aldus de definitieve bevindingen van het onderzoek naar de zgn. 'Geen Stijl IP-checker op GeenCommentaar.nl (z2008-01174), 27 oktober 2008.

18 De website van het CBP noemt o.a.: Koorn et al, 2004; Van Blarkom, Borking & Olk (eds.) 2003; Kenny & Borking, 2002; CBP 2002; Borking & Raab, 2001.

In het verlengde daarvan is denkbaar dat deze beweegredenen wellicht ook liggen in wat tegenwoordig allemaal kan met IP-adressen en andere identifiers. In de richtsnoeren wordt daarover iets interessants gezegd:

"Ten slotte is van belang dat op basis van het IP-adres beslissingen kunnen worden genomen over de toegang tot bepaalde informatie, zonder dat een dienstverlener op internet überhaupt enige moeite hoeft te doen om zelf persoonsgegevens te verbinden aan een IP-adres. Denk bijvoorbeeld aan onderscheid naar geografische herkomst bij de toegang tot en de presentatie van (delen van) websites. Ook het registreren en eventueel op internet publiceren van IP-adressen van bezoekers van een website of deelnemers aan een discussieforum valt dus onder het bereik van de Wbp."

Er wordt, zo begrijp ik, enerzijds opgemerkt dat persoonsgegevens kunnen worden verbonden aan IP-adressen, waarmee wordt gesuggereerd dat IP-adressen a priori geen persoonsgegevens hoeven zijn, maar dat kúnnen worden als er een verband wordt gelegd met persoonsgegevens. Anderzijds lijkt te worden gezegd dat IP-adressen, ook als ze eigenlijk geen persoonsgegevens zijn, niettemin onder de werkingssfeer van de Wbp zouden moeten worden gebracht. Dit omdat ze zouden kunnen worden gebruikt om 'beslissingen' te nemen over nog niet geïdentificeerde of identificeerbare internetgebruikers.

Er staat niet wat er staat, dichtte Nijhoff. En ik lees er misschien meer in dan wordt bedoeld. Dat doet er evenwel niet aan af dat aan de hand van IP-adressen inderdaad beslissingen kunnen worden genomen met betrekking tot geïndividualiseerde, maar niettemin nog ongeïdentificeerde of onidentificeerbare internetgebruikers. Zeg: de internetgebruiker van wie is vastgesteld dat hij eind oktober jl. in de executive lounge te Geneve Cointrin International gebruik maakte van IP-adres 194.209.131.192.

Allereerst kan dergelijke informatie worden gebruikt om onderscheid te maken tussen internetgebruikers naar geografische locatie, bijvoorbeeld om te voorkomen dat voornoemde internetgebruiker bij iTunes zijn muziek niet in euro's afrekent, maar met de voor hem voordelige dollars.[19] Verder is voorstelbaar dat Apple en wellicht ook Nike om andere redenen belangstelling hebben voor deze, vooralsnog ongeïdentificeerde maar wel geïndividualiseerde internetgebruiker. Zeker als uit de analyse van zijn (of haar) internetactiviteiten zou blijken dat hij (of zij) bovengemiddeld is geïnteresseerd in grote hardloopevenementen, trendgevoelige draagbare muziekspelers, en daarbij met enige regelmaat vliegreizen binnen Europa maakt. Waarom maakt het voor het sportmerk of elektronicabedrijf niet uit dat deze gebruiker (vooralsnog?) niet is geïdentificeerd? Omdat het voor hen voldoende is als zij op de eigen websites, en die van anderen, aan deze specifieke gebruiker de juiste web-advertenties of banners kunnen laten zien. Bijvoorbeeld over de nieuwste generatie (Air Force) loopschoenen en een iPod Sport Kit.

19 Denk ook aan: differentiëren naar geografische locatie van internetgebruikers en het voorkomen van parallel-import; vgl Bloemen-Patberg, Zwenne & De Weerd 2009, p. 79.

Daarvoor hoeft de gebruiker niet te zijn geïdentificeerd, maar alleen geïndividualiseerd. En daarvoor is een IP-adres toereikend.

Er is meer mogelijk. Wat in de online reclamewereld wordt aangeduid als behavourial targeting of profiling – het met onder meer IP-adressen in kaart brengen van de voorkeuren van geïndividualiseerde internetgebruikers[20] – kan in andere contexten worden toegepast, soms met ernstigere consequenties dan het vertonen van banners. Aangenomen mag worden dat bijvoorbeeld auteursrechtorganisaties belangstelling hebben voor geïndividualiseerde downloaders. En dat niet alleen om deze op enig moment te identificeren, maar ook om alvast het dossier op te bouwen en vast te leggen wat deze geïndividualiseerde internetgebruikers allemaal doen. Ook denkbaar is dat deze rechthebbenden van ISP's gedaan krijgen dat wordt overgegaan tot het afsluiten van de niet door hen geïdentificeerde, maar wel geïndividualiseerde abonnees die gebruik maken van de door hen als verdachte aangemerkte IP-adressen.[21] Ook in deze situatie volstaan IP-adressen en is niet per se nodig dat de identiteit van de abonnees (al?) bekend is.

Er is weinig fantasie voor nodig om in het verlengde daarvan andere situaties te bedenken waarin er aanleiding is om internetgebruikers te individualiseren met IP-adressen. Wat te denken van de opsporingsautoriteiten die een zaak 'opbouwen' over bijvoorbeeld dierenliefhebbers woonachtig in kraakpanden en met een bijzondere belangstelling voor adressen van politici en de receptuur van (verf)bommen? Wat te zeggen van de wens van sommige regimes om informatieposities op te bouwen tegen de bezoekers van hen onwelgevallige websites, of tegen subversieve bloggers en de lezers van hun blogberichten, enz.

Ik wil maar zeggen. Ook als er nog geen sprake is van identificeerbaarheid zijn er talloze goede en minder goede redenen om aan de hand van IP-adressen gedetailleerde profielen aan te leggen van geïndividualiseerde maar niettemin ongeïdentificeerde internetgebruikers. In termen van privacy heeft dit implicaties, ook als er volgens de gangbare definitie nog geen sprake is van identificeerbaarheid. Voor een toezichthouder van wie de bevoegdheid is beperkt tot persoonsgegevens, is de begrijpelijke eerste reflex dan om het persoonsgegevensbegrip zo te interpreteren dat IP-adressen hoe dan ook daaronder vallen. En om zodoende individualiseren gelijk te stellen met identificeren.[22] En dat alles waarschijnlijk met als achterliggende gedachte dat een teveel aan privacywaarborgen is te verkiezen boven te weinig.

---

20 Koeter 2009.

21 Zo is het naar verluid wel gebeurd dat een heel studentenhuis werd afgesloten omdat er één gebruiker iets had gedaan wat volgens de ISP (of anderen?) niet door de beugel kon.

22 In die zin laat Hustinx, de voorzitter van de Europese privacytoezichthouder, zich uit in een kort webinterview op ZDnet: "identifiable in the sense of personal data is singling someone out; we don't need to name name and address". http://news.zdnet.co.uk/security/0,1000000189,39540137,00.htm.

De toekomst van privacywetgeving (Privacywet 2.0)

De gedachte waarmee de vorige paragraaf eindigde is niet onsympathiek. Als het gaat om de bescherming van de persoonlijke levenssfeer is een teveel aan waarborgen te verkiezen boven te weinig. En, gelet op wat er met IP-adressen kan, is er wellicht veel voor te zeggen om op de een of andere manier beperkingen te stellen aan het gebruik van IP-adressen en andere gegevens, waarmee internetgebruikers worden geïndividualiseerd – ook als die gegevens nog niet, of nog niet voor iedereen, als persoonsgegevens zijn aan te merken.

In dergelijke beperkingen voorziet de Wbp niet, tenzij wordt uitgegaan van een zo extensieve interpretatie van het persoonsgegevensbegrip dat IP-adressen per definitie daaronder vallen. De vraag is of daarom de privacywetgeving van de toekomst (zeg: Privacywet 2.0) inderdaad moet uitgaan van een persoonsgegevensbegrip dat vanzelfsprekend ook IP-adressen omvat, en daarmee ook andere identifiers (bijvoorbeeld IMSI of IMEI-nummers, of RFID-nummers enz.).

Er zijn verschillende redenen waarom wij dit niet moeten willen. Wat mij betreft ligt de belangrijkste daarvan in het voorkomen dat de Wbp als privacywet betekenis verliest. Een extensieve interpretatie leidt ertoe dat de werkingssfeer van de wet wordt opgerekt tot ver voorbij wat nog werkbaar is. Een dergelijke interpretatie impliceert dat bij de toepassing van het identificeerbaarheidscriterium wordt voorbijgegaan aan zowel de objectivering naar de redelijk toegeruste gegevensverwerker ('wat in de gegeven situatie redelijkerwijs mag worden verwacht') als de subjectivering naar diens bijzondere expertise ('expertise', 'contacten', 'technische outillage' enz.).

En dat brengt onvermijdelijk met zich mee dat veel (heel erg veel) meer gegevens onder de werkingssfeer van de wet komen te vallen. En, wat belangrijker is, dat er dan géén hanteerbaar criterium meer is waarmee kan worden bepaald wat géén persoonsgegeven (meer) is. Als er al kan worden gesproken van identificeerbaarheid als op enig moment er de mogelijkheid zou kunnen zijn dat een individu wordt geïdentificeerd, verliest identificeerbaarheid als criterium onderscheidend vermogen. Alles wat dan op enig moment kan leiden tot identificatie is daarmee een persoonsgegeven, althans moet als zodanig worden behandeld, wat op hetzelfde neerkomt. Het risico dat ik zie is dat toepassing van de wet dan toevallig wordt, en de naleving en de handhaving willekeurig.

In het verlengde daarvan zijn er nog meer redenen waarom de door toezichthouders verdedigde extensieve uitleg van het persoonsgegevensbegrip onverstandig is. Op dit moment, uitgaande van een redelijk genuanceerde interpretatie wordt de werkingssfeer van de wet vaak al ervaren als onbegrensd.[23] Als ervan uit wordt gegaan dat IP-adressen altijd als persoons-

23 Vgl. bijv. Van der Horst 2002; De Hert & Gutwirth, 2004; Zwenne et al, 2007, p. 12, 61, 64-68, 96, 137, 157 en 168.

gegevens moeten worden aangemerkt, valt daarop weinig meer af te dingen. Als dat nu al niet het geval is, dan toch in elk geval na de introductie van de nieuwe generatie van IP-adressen (IPv6), waarmee de voorraad van IP-adressen naar verluid voldoende is om ieder individueel atoom op aarde een eigen nummer te geven.[24]

Voor het toezicht is relevant dat de extensieve interpretatie zoveel rechtsonzekerheid met zich brengt dat handhavingsmaatregelen het risico lopen te stuiten op het lex certa-beginsel, het beginsel dat alleen sancties mogen worden opgelegd met betrekking tot overtredingen van normen die voldoende voorzienbaar en duidelijk zijn.[25] Ook relevant is wellicht dat de extensieve interpretatie een streep lijkt te halen door de ontwikkeling van privacy by design en privacy enhancing technologies, en alle inspanningen die daarvoor, niet in de laatste plaats door de toezichthouder, zijn gedaan.[26] Als IP-adressen per definitie als persoonsgegevens worden aangemerkt, of als zodanig moeten worden behandeld, heeft het weinig zin meer om de technische en organisatorische maatregelen te nemen om gegevensverwerkingen zo in te richten dat er geen sprake meer is van identificeerbaarheid. Althans, dergelijke maatregelen leiden dan niet tot een vermindering van de compliance-kosten, wat een belangrijke reden is om daarin te investeren.

Verder geldt dat een te extensieve interpretatie ingaat tegen andere uitingen van toezichthouders[27] en ook tegen de nog schaarse rechtspraak over IP-adressen,[28] en als zodanig de geloofwaardigheid van het toezicht geen goed doet. Ook niet onbelangrijk zijn uitvoeringsproblemen waartoe deze interpretatie aanleiding geeft, bijvoorbeeld waar het gaat om het inzagerecht, de informatieplicht, de meldingsplicht of de internationale doorgifte van de gegevens.[29] En daarbij is het maar de vraag of de privacybescherming, mede gelet op het voorgaande, uiteindelijk wel is gebaat bij deze extensieve interpretatie.

---

24 IPv4 kent 32 bits en ondersteunt iets meer dan 4 miljard (om percies te zijn 4.294.967296) IP-adressen; IPv6 kent 128 bits en ondersteunt dus het astronomische aantal van precies 3 40.282.366.920.938.463.463.374.607.431.768.211.456 IP-adressen.

25 Zie o.a. EHRM 25 mei 1993, ECRM Series A, Vol. 260; EHRM 27 september 1995, *NJ* 1996, 49; Rb.'s-Gravenhage 23 december 1998, *JB* 1999, 57; ABRvS 8 december 2004, AB, 2005, 44; ABRvS 20 november 2002, *AB* 2003, 173; CBb 24 augustus 2006, *AB* 2007, 321; CBb 20 december 2007, *AB* 2008, 56; zie ook *Kamerstukken II* 2003–04, 29 702, nr. 3, p. 86

26 Zie voetnoot 16.

27 In aanvulling op de reeds genoemde uitingen van CBP en de werkgroep kan worden gewezen op de zgn. Good practice note – Collecting personal information using websites, van 5 juni 2007, waarin de privacytoezichthouder in het Verenigd Koninkrijk overweegt dat dynamische IP-adressen niet vanzelfsprekend onder de UK Data Protection Act 1998 vallen http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/collecting_personal_information_from_websites_v1.0.pdf; zie daarover: Bloemen-Patberg, Zwenne & De Weerd 2009, p. 89.

28 Zie bijv. Ambtsgericht München, Geschäftsn: 133 C 5677/08, 30 september 2008; in voetnoot 15 noemde ik al Cour d'appel de Paris 13ème chambre, section B Arrêt du 27 avril 2007 en section A Arrêt du 15 mai 2007.

29 Vgl. Bloemen-Patberg, Zwenne & De Weerd 2009, p. 90-91.

Het punt is denk ik wel gemaakt. Blijft de vraag of er, gelet op wat er allemaal kan met IP-adressen, toch niet op de een of andere manier beperkingen zouden moeten worden gesteld aan het gebruik ervan, ook als er nog geen natuurlijke personen mee kunnen worden geïdentificeerd. Ik ben geneigd deze vraag bevestigend te beantwoorden. De privacy-implicaties van de technologieën als behavourial targeting, profiling, deep-packet sniffing en data mining lijken ingrijpend genoeg te zijn om daarover ten minste serieus na te gaan denken. Ik zoek dergelijke beperkingen echter niet in de Wbp maar in de telecomwetgeving. Daarin zijn al regels gesteld voor IP-adressen en andere identifiers. Meer daarover in de volgende, voorlaatste paragraaf van deze bijdrage.

Mijn voorstel voor regulering van IP-adressen

In termen van de telecomwetgeving worden IP-adressen aangemerkt als verkeersgegevens, omdat ze worden gebruikt om verkeer via elektronische communicatie (telecom, internet) over te brengen naar computers, routers, PDA's, iPhones en andere devices.[30] Voor verkeersgegevens, en dus ook voor IP-adressen, geldt een aantal specifieke regels, voorzover met deze gegevens natuurlijke of rechtspersonen kunnen worden geïdentificeerd. De hoofdregel is dat telecom- en internetaanbieders verkeersgegevens moeten verwijderen of anonimiseren, zodra ze niet meer nodig zijn voor het overbrengen van de communicatie en de facturering daarvan.[31] Uitzonderingen betreffen het met toestemming van de desbetreffende abonnee gebruiken van de gegevens voor marktonderzoek en de verlening van value added services, alsmede de bewaarplicht ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven.[32]

Er staan in telecomwetgeving geen regels voor IP-adressen waarmee geen natuurlijke of rechtspersonen kunnen worden geïdentificeerd. Er is dus geen regel op grond waarvan bijvoorbeeld ISP's en andere internetdienstverleners (zoekdiensten, ad services enz.) beperkt worden in het gebruik van IP-adressen waarmee geen natuurlijke personen kunnen worden geïdentificeerd. Wel kent de telecomwetgeving regels voor andere, tot op zekere hoogte met IP-adressen vergelijkbare gegevens of identifiers. Voor telefoonnummers van natuurlijke personen is bepaald dat deze alleen in telefoongidsen en informatiediensten mogen worden opgenomen met toestemming van de desbetreffende natuurlijke personen.[33] Ook is bepaald dat de telefoonnummers alleen met toestemming van de desbetreffende natuurlijke personen

30 In een bijlage bij de Telecommunicatiewet is de lijst opgenomen met de verplicht door ISP´s te bewaren verkeersgegevens, waaronder IP-adressen.

31 Art. 11.5, eerste lid, Tw.

32 Art. 13.2a, tweede lid, Tw jo. onderdeel A(c) van de bijlage bij deze bepaling; zie daarover Schmidt & Zwenne 2005; Zwenne & Schmidt 2008.

33 Art. 11.6, tweede lid, Tw.

mogen worden gebruikt voor andersoortige diensten, waarbij vooral moet worden gedacht aan de diensten waarmee aan de hand van het vaste of mobiele telefoonnummer de bijbehorende abonnee kan worden gezocht en gevonden. Op grond dit verbod van 'reversed search' of 'omgekeerd zoeken' is het de telefoonaanbieder niet toegestaan anderen in staat stellen om aan de hand van het telefoonnummer de identiteit te achterhalen van de abonnee die van dat nummer gebruik maakt. De telecomwetgeving voorziet daarmee in waarborgen ter voorkoming van het ongewenst, althans zonder toestemming, identificeren van natuurlijke personen met behulp van telefoonnummers.[34]

Eenzelfde regeling is voorstelbaar als het gaat om IP-adressen. Een eenvoudige regel zou kunnen zijn dat het ISP's niet is toegestaan om anderen in staat te stellen aan de hand van IP-adressen zomaar, althans zonder toestemming, de identiteit te achterhalen van de natuurlijke personen die daarvan gebruik maken. Zo een regel zou het logisch complement kunnen zijn van de bepalingen voor verkeersgegevens. Enerzijds zijn ISP's volgens de reeds geldende regels[35] gehouden IP-adressen in beginsel zo snel mogelijk te anonimiseren of te verwijderen. Zolang de IP-adressen niet zijn geanonimiseerd is het hen anderzijds, volgens mijn voorgestelde regel, niet toegestaan om zomaar zonder toestemming of andere toereikende grondslag anderen in staat te stellen daarmee de abonnees te identificeren.

In aanvulling kan ook worden gedacht aan een regeling vergelijkbaar met die voor nummerherkenning. In de telecomwetgeving is bepaald dat abonnees verschillende rechten hebben met betrekking tot het bekend worden van het nummer waarmee zij bellen. Abonnees hebben het recht om nummerherkenning uit te zetten en anoniem te bellen — dit behoudens uitzonderingen in de sfeer van alarmnummers, anti-stalking en opsporing en vervolging.[36] Een vergelijkbare regel is met enige aanpassingen denkbaar voor IP-adressen. Er zou kunnen worden bepaald dat ISP's aan hun abonnees een faciliteit moeten aanbieden waarmee het mogelijk wordt om het IP-adressen af te schermen voor derden. Als abonnees daarvan gebruik maken, kan dat natuurlijk betekenen dat allerlei internetdiensten niet of niet prettig werken. Maar in elk geval hebben de abonnee dan de keuze, zoals zij dat ook al hadden als zij gebruik maken van telefoondiensten.[37]

---

34 Opgemerkt moet worden dat zowel CBP als OPTA tot dusver het omgekeerdzoek-verbod niet echt willen handhaven. Dit omdat, in de woorden van de telecomtoezichthouder, overtreding van het verbod 'op zichzelf genomen niet als inbreuk op de persoonlijke levenssfeer wordt ervaren', zie OPTA-besluit 17 oktober 2007 (OPTA/IPB/2007/202118). Het CBP-besluit, waarin ook werd afgezien van handhaving, is niet gepubliceerd maar wordt wel genoemd in het CBP Jaarverslag 2008, p. 18 en 41.

35 Art. 11.5 Tw

36 Art. 11.9, eerste lid, onder a, jo. Art. 11.10 en 11.11 Tw.

37 Er zijn op internet verschillende typen van anonymous en pseudomynous remailers beschikbaar, maar de gebruiksvriendelijkheid daarvan laat veel te wensen over. De betrouwbaarheid ervan is niet altijd evident.

Afsluiting

Het mag duidelijk zijn. Wat mij betreft is het onverstandig is om het persoonsgegevensbegrip extensiever te interpreteren en al uit te gaan van identificeerbaarheid als er de theoretische mogelijkheid is dat er met een bepaald gegeven door iets of iemand een natuurlijke persoon zou kunnen worden geïdentificeerd. Wat mij betreft niet alleen onverstandig, maar ook onlogisch, omdat de telecomwetgeving veel meer voor de hand liggende aanknopingspunten biedt.

Onduidelijk is of er meer nodig is. Er worden vanuit heel verschillende achtergronden vraagtekens geplaatst bij de uitgangspunten van privacywetgeving, meer in het bijzonder waar het gaat om het persoonsgegevensbegrip en het identificeerbarheidscriteriumm. Van den Hoven[38] bijvoorbeeld pleit voor een bredere benadering dan die waarbij wordt uitgegaan van beschrijvingen die verwijzen naar individuen ('referential use'). Er zou ook op de een of andere manier moeten worden uitgegaan van beschrijvingen die niet verwijzen naar individuen, maar niettemin 'identity-relevant' zijn:

> "the referential reading of personal data, identity and identifiability of the EU data-protection laws leads to an unduly narrow construal of moral constraints on the use of personal data."

Vanuit een andere achtergrond stelt Prins aan de orde dat privacywetgeving te weinig aandacht heeft voor de veranderende betekenis van 'identificeren' en 'identiteiten' in de informatiesamenleving,[39] alsook dat de bestaande privacywetgeving onvoldoende waarborgen biedt om individuen te beschermen tegen de in bepaalde contexten opgelegde identiteiten.[40]

Ook andere auteurs vragen aandacht voor de uitgangspunten van de privacywetgeving en de privacy-implicaties van de verwerking van gegevens die eigenlijk geen persoonsgegevens zijn, en die dus niet door de Wet bescherming persoonsgegevens worden geadresseerd.[41] Voor deze bijdrage, die al veel meer woorden telt dan de redactie van dit boek heeft bepaald, volsta ik met een verwijzing naar Schmidt.[42] In zijn oratie wijst hij erop dat IP-adressen niet de gebruikers identificeren maar de computer waarvan deze gebruik maken. Maar dat doet er niet aan af, zo zet hij uiteen, dat het verzamelen van IP-adressen en talloze andere gegevens zal leiden tot 'mega-informatieposities' die op de een of andere wijze regulering behoeven, als wij de kwaliteit van rechtsstaat en privacybescherming serieus willen nemen:

---

38 Van den Hoven 2008.
39 Prins 2004a, Prins 2004b.
40 Prins 2009, p. 42.
41 Zie bijv. De Hert et al. 2007, Kindt & Van der Hof 2009, Marbus et al. 2009, Hoving 2008.
42 Schmidt 2004, p. 31.

> "De vraag hoe we informatieposities reguleren is van belang voor de kwaliteit van onze rechtsstaat. In die zin vormen de grote, ik zou bijna zeggen mega informatieposities van de kennisbovenbazen zowel kansen voor bescherming als voor bedreiging. Het op de individu gerichte grondrecht op privacy komt in dit spanningsveld niet erg goed uit de verf."

Een en ander krijgt praktische betekenis in de discussie over IP-adressen. Het komt mij voor dat deze discussie erbij is gebaat als zo af en toe concrete voorstellen worden gedaan. Deze bijdrage moet in dat licht worden gezien.

Verwijzingen

Van Blarkom, Borking & Olk 2003
G.W. van Blarkom, J.J. Borking en J.G.E. Olk (eds.), *Handbook of Privacy and Privacy-Enhancing Technologies: The case of Intelligent Software Agents*, Den Haag 2003.

Bloemen-Patberg, Zwenne & De Weerd 2009
A. Bloemen-Patberg, G-J. Zwenne en 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, pp. 79-97.

Borking & Raab 2001
J. Borking en C. Raab, 'Laws, PETs and Other Technologies for Privacy Protection', *Journal of Information, Law and Technology* 2001/1.

CBP 2002
CBP, *Mag het een bitje minder zijn*? Den Haag 2002.

Van Esch 2008
R.E. van Esch, *Juridische aspecten van elektronische handel*, Deventer 2008.

Van Esch & Blok 2007
R.E. van Esch en P. Blok, 'Privacy en elektronische handel op het internet', in: Berkvens & Prins (red.) *Privacyregulering in theorie en praktijk* Kluwer, Deventer 2007.

De Hert et al. 2009
P.J.A. de Hert et al., 'De WBP na de Dexia-uitspraken', in: *P&I* 2007/4, bldz. 147-157

De Hert & Gutwirth 2004
P. de Hert en 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.

Van der Horst 2004
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, p. 113.

Van den Hoven 2008
J. van den Hoven, 'Information Technology, Privacy, and the Protection of Personal Data', in: Van den Hoven & Weckert (eds.), *Information Technology and Moral Philosophy*, New York 2008, p. 301-319.

Hoving 2008
E. Hoving, 'Modellering van persoonsgegevens en groepsprofielen', in: *P&I* 2008/6, p. 273-280.

Kenny & Borking 2002
S. Kenny en J.J. Borking, 'The Value of Privacy Engineering', *Journal of Information, Law and Technology*, 2002/1.

Kindt & Van der Hof
E. Kindt en S. van der Hof, 'Identiteitsgegevens en -beheer in een digitale omgeving: een juridische benadering', in: *Computerrecht* 2009/2, p. 52/60.

Klitou 2008.
D.G. Klitou 'Backscatter body scanners – A strip search by other means', *Computer Law & Security Report* 2008/24, pp. 316–325.

Koeter 2009
J. Koeter, 'Behavioral targeting en privacy: een juridische verkenning van internet gedragsmarketing', *Tijdschrift voor internetrecht* 2009(4), p. 104-111.

Koorn 2004
R. Koorn et al, *Privacy Enhancing Technologies: Witboek voor beslissers*, Ministerie van Binnenlandse Zaken en Koninkrijkrelaties 2004.

Marbus et al. 2009
R.C.P. Marbus et al., 'Identiteit en openbaarheid in sociale online omgevingen', in: *Computerrecht* 2009/2, p. 64-68.

Prins 2004a
J.E.J. Prins, 'Technologie en de nieuwe dilemma's rond identificatie, anonimiteit en privacy', *Justitiële Verkenningen*, 2004-8, p. 34-47

Prins 2004b
J.E.J. Prins, 'The Propertization of Personal Data And Identities', *EJCL*, Vol. 8.3 October 2004.

Prins 2009
J.E.J. Prins, 'Gezocht: uw identiteit', *Computerrecht* 2009/2, p. 42.

Schmidt 2008
A.H.J. Schmidt, *Bedreigen computers ons rechtssysteem?* 2008.

Schmidt & Zwenne 2005
A.H.J. Schmidt en G-J. Zwenne, 'Recht en risico. Kanttekeningen bij het voorstel voor een richtlijn over de bewaring van telecommunicatie-verkeersgegevens' *Mediaforum* 2005/9, p. 292-302.

Zwenne et al. 2007
G-J. Zwenne et al, *Eerste fase evaluatie Wet bescherming persoonsgegevens. Literatuuronderzoek en knelpuntenanalyse*, Den Haag 2007.

Zwenne & Schmidt 2008
G-J. Zwenne en A.H.J. schmidt, 'Opmerkingen bij het wetsvoorstel Wet bewaarplicht telecommunicatiegegevens', *Mediaforum* 2008/7-8, p. 278-385.