Wie bepaalt wat gebeurt met IP adressen en verkeers- en locatiegegevens?

Bloemen-Patberg, A.; Zwenne, G.J.; Weerd, T. de; Visser E.N.M., Weij M.

4 Wie bepaalt wat gebeurt met IP adressen en verkeers- en locatiegegevens?

A. Bloemen-Patberg, G-J. Zwenne & T. de Weerd

4.1 Inleiding

Wie heeft zeggenschap over uw gegevens als u gebruik maakt van internet? Wie is eigenaar van de gegevens over uw surfgedrag of over uw zoekopdrachten? Wie bepaalt wat er gebeurt met de gegevens over de omvang of bestemmingen van uw e-mailberichten? Wat mag er met deze gegevens wél of niet worden gedaan, en wat hebben de internetgebruikers daarover nog te zeggen?

Deze en andere vragen worden beantwoord binnen de kaders van wat wel wordt aangeduid als de privacywetgeving. Of, om het preciezer te zeggen, de wetgeving betreffende de verwerking van persoonsgegevens: de Wet bescherming persoonsgegevens ("Wbp").[125] Verder moet bij de beantwoording van deze vragen worden uitgegaan van de meer specifieke regels voor verkeers- en locatiegegevens, waarmee de gegevens over internet- en telefoongebruik worden bedoeld. Deze regels staan in de Telecommunicatiewet ("Tw").

In dit hoofdstuk worden deze kaders besproken. Eerst wordt ingegaan op de betekenis van de Wbp als het gaat om het opslaan en verwerken van IP adressen, dat wil zeggen de gegevens waarmee de identiteit van apparaten (en daarmee mogelijk de identiteit van gebruikers) op internet bekend wordt gemaakt (§2). Vervolgens worden de meer specifieke regels voor verkeers- en locatiegegevens besproken en de gevolgen die deze regels hebben voor de zeggenschap over

125 De aanduiding 'privacywetgeving' is niet erg precies. Enerzijds valt onder deze wetgeving veel meer dan de bescherming van persoonsgegevens – denk aan roddeljournalistiek; anderzijds is het vaak maar de vraag of met de door de wet voorgeschreven regels ter bescherming van persoonsgegevens altijd een privacybelang is gediend.

verkeers- en locatiegegevens (§3). Aansluitend volgteen korte slotbeschouwing met enige conclusies en afsluitende opmerkingen (§4).[126]

4.2 Wie heeft zeggenschap over IP adressen?

4.2.1 Inleiding

Met IP adressen kan Apple tegengaan dat Europese consumenten muziek en video's aanschaffen via de Amerikaanse iTunes-dienst. IP adressen maken het mogelijk dat in China de websites van Falung Gong niet kunnen worden bezocht. Uit deze, en talloze andere, voorbeelden[127] wordt duidelijk dat wie kan beschikken over IP-adressen daarmee kan controleren (sturen) wat gebruikers op het internet kunnen doen, welke websites zij kunnen bezoeken of welke files zij kunnen downloaden, enzovoorts.

Dezelfde voorbeelden laten zien dat gebruikers er belang bij kunnen hebben om hun identiteit, nationaliteit of woonplaats niet bekend te maken, en ook dat zij om die reden wellicht zelf willen kunnen bepalen wat er gebeurt met de IP adressen die daarover iets zeggen. En als zij dat niet kunnen, dan hebben zij er in elk geval belang bij dat ze kunnen weten wat er met hun IP adressen wordt gedaan en dat de verwerking daarvan op een zorgvuldige wijze gebeurt.

Voor de vraag of de privacywetgeving, in Nederland dus met name de Wbp, dergelijke waarborgen kan bieden is bepalend of en zo ja in hoeverre IP adressen kunnen worden aangemerkt als persoonsgegevens in de zin van die wet. Om die vraag te beantwoorden is evenwel eerst van belang te zien wat IP adressen eigenlijk zijn.

4.2.2 Wat zijn IP adressen?

Elk apparaat dat met het internet is verbonden (pc, handheld, gameconsole, pda, server, routers, enz.) krijgt een tijdelijk of permanent uniek nummer toegewezen

126 Zonder af te doen aan de gezamenlijke verantwoordelijkheid van de auteurs voor dit hoofdstuk wordt opgemerkt dat het auteurschap van §4.2 – 4.6 vooral ligt bij Annemarie en Thomas en dat van §4.7 – 4.12 bij Gerrit-Jan.

127 Een aardige indruk kan worden verkregen door in Google of Wikipedia te zoeken op «IP-blocking», «IP-address + censorship» of bijvoorbeeld «China + Google + Censorship» of «iTunes + price discrimination».

dat bestaat uit vier sets van maximaal drie cijfers, bijvoorbeeld 216.239.59.104.[128] Met dit nummer, het zogenaamde Internet Protocol Address of IP adres, kan het apparaat bereikbaar worden gemaakt voor andere apparaten, en kan het apparaat worden geïdentificeerd.

IP adressen voor apparaten van internet-gebruikers worden normaliter toegewezen door Internet Service Providers of ISP's. Er bestaan twee soorten IP adressen: statische en dynamische. Een statisch IP adres is aan een server of computer gekoppeld; iedere keer als de computer of server zich op het internet begeeft, wordt hetzelfde IP adres gebruikt. Dynamische IP adressen worden voor een bepaalde duur aan een computer toegewezen en zijn vaak weer anders[129]

4.3 Is een IP adres (altijd) een persoonsgegeven?

Iedere keer dat een internetgebruiker zich op het internet begeeft, wordt het IP adres van zijn apparaat zichtbaar, bijvoorbeeld voor de website die wordt bezocht of het netwerk waarop wordt ingelogd. De vraag is of dit enkele IP adres al kan worden gezien als een persoonsgegeven in de zin van de Wbp.

Het begrip 'persoonsgegeven' wordt in artikel 2 (a) van de Privacyrichtlijn 95/46/EG, die ten grondslag ligt aan de Wbp, op de volgende wijze omschreven:

> *"any information relating to an identified or identifiable natural person".*

In artikel 1 (a) van de Wbp wordt dit op de volgende wijze vertaald:

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

Uit deze omschrijvingen kan worden afgeleid dat het voor de vraag of een IP adres een persoonsgegeven is, doorslaggevend is of het mogelijk is om daarmee een bepaalde natuurlijke persoon te identificeren. Over deze, voor de toepassing van de Wbp beslissende vraag, hebben zowel het College Bescherming Persoons-

128 Een van de IP adressen die leiden naar http://www.google.nl.

129 Aan een dynamisch IP adres wordt een releasetijd gekoppeld door de verstrekkende DHCP-server van de ISP. Dat kan bijvoorbeeld een maand zijn: wordt de pc binnen die tijd op het internet gebruikt, dan houdt de pc hetzelfde IP adres. Zo kan een pc járenlang hetzelfde dynamische IP adres hebben.

gegevens ("CBP") als de Artikel 29 Werkgroep[130] ("Art. 29 WG") zich meerdere keren uitgelaten.

Het CBP en de Art. 29 WG beperken zich bij de beantwoording van deze vraag vooral tot dynamische IP adressen. Van statische IP adressen, die vast aan een bepaalde computer of server zijn verbonden, wordt kennelijk min of meer aangenomen dat het persoonsgegevens zijn. Daarbij gaan zij er gemakshalve aan voorbij dat veel IP adressen zijn gerelateerd aan servers, routers en andere computerhardware die niet per sé rechtstreeks door natuurlijke personen worden gebruikt.

Artikel 29 Werkgroep
De Art. 29 WG heeft zich in een aantal van deze aanbevelingen uitgelaten over het IP adres. In februari 1999, in het werkdocument "Verwerkingen van persoonsgegevens op het internet"[131], stelde de Art. 29 WG dat het internet een uitdaging voor de bescherming van persoonsgegevens en het recht op privacy is. De Art. 29 WG nam daarbij toen al het volgende aan:

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

Een tweede keer dat de Art. 29 WG expliciet stelt dat IP adressen als persoonsgegeven moeten worden gezien is in het werkdocument "Privacy op internet – Een geïntegreerde EU-aanpak van onlinegegevensbescherming", van 21 november 2000[132]. In dit werkdocument wordt gesteld dat het buiten kijf staat dat IP adressen in elk geval voor ISP's en beheerders van lokale netwerken persoonsgegevens zijn. De reden hiervoor is dat de internetaanbieders en beheerders systematisch de datum, het tijdstip, de duur en het verstrekte (dynamische) IP adres vastleggen. Voor derden is dit anders, zo stelde de werkgroep. Zij kunnen het IP adres namelijk niet koppelen aan andere gegevens die de internetgebruikers kunnen identificeren[133].

---

130 De Art. 29 WG is het op grond van art. 29 van de Privacyrichtlijn ingestelde adviesorgaan dat (vooral) bestaat uit vertegenwoordigers van nationale toezichthouders en dat met grote regelmaat adviezen en opinies over de bescherming van persoonsgegevens publiceert (http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm).

131 Article 29 Data Protection Working Party, *Processing of Personal Data on the Internet*, WP 16 d.d. 23 februari 1999 (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/ 1999/wp16nl.pdf).

132 Article 29 Data Protection Working Party, Privacy on the Internet" – An integrated EU Approach to On-line Data Protection WP d.d. 21 november 2000 (http://ec.europa.eu/ justice_home/fsj/privacy/docs/wpdocs/2000/wp37nl.pdf).

133 De Artikel 29 Werkgroep maakt hierbij wel de kanttekening dat identificatie van internetgebruikers die een statisch IP adres gebruiken, gemakkelijker is.

Een en ander doet er volgens de Art. 29 WG niet aan af dat het toch vaak mogelijk om de gebruiker van het IP adres te identificeren. Dit kan door het IP adres te koppelen aan andere gegevens die over deze gebruiker zijn verkregen, bijvoorbeeld via cookies[134] of door analyses van grote gegevensbestanden (data mining[135]). Om deze redenen gaat de Art. 29 WG ervan uit dat grote hoeveelheden persoonsgegevens, waaronder ook IP adressen, op het internet worden verwerkt.

Op 20 juni 2007 heeft de Art. 29 WG een uitgebreide opinie gegeven over het begrip persoonsgegevens[136], waarin zij in het kader van de kwalificatie van een IP adres een en ander herhaalt en verder onderbouwt. Dit kwam aan de orde in het kader van het derde element van de definitie van persoonsgegeven, namelijk het element "geïdentificeerd of identificeerbaar". In overweging 26 van de Privacyrichtlijn wordt over dit element het volgende overwogen:

> *"Overwegende dat de beschermingsbeginselen moeten gelden voor elk gegeven betreffende een geïdentificeerde of identificeerbare persoon; dat, om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde persoon te identificeren;*
> *dat de beschermingsbeginselen niet van toepassing zijn op gegevens die op zodanige wijze anoniem zijn gemaakt dat de persoon waarop ze betrekking hebben niet meer identificeerbaar is;"*

Dit houdt in, aldus de Art. 29 WG, dat een slechts hypothetische mogelijkheid om iemand te onderscheiden niet voldoende is om die persoon als identificeerbaar te beschouwen.

Om te beoordelen of sprake is van "redelijkerwijs in te zetten middelen" moet rekening worden gehouden met alle relevante omstandigheden van het geval. Als voorbeeld geeft de Art. 29 WG de situatie dat een houder van een auteursrecht IP adressen verzamelt of laat verzamelen waarvan wordt vermoed dat door de

---

134 Een *cookie* is een tekstbestandje dat door veel websites automatische op de computer van de bezoeker wordt geplaatst. In de *cookie* wordt onder andere de locatie, handelingen en voorkeuren van de bezoeker op de website bijgehouden en, indien van toepassing, ook de ingevulde gegevens. Ook worden in een *cookie* de datum en tijd opgeslagen van het moment dat hij op de computer is geplaatst, en welke IP adres de computer toen had. De volgende keer dat de internetgebruiker de desbetreffende website bezoekt, leest de website deze informatie uit de *cookie*, en past de website zichzelf daarop aan.

135 *Data mining* is het hergebruiken van beschikbare data. Getracht wordt om op een geautomatiseerde manier patronen en relaties te ontdekken in grote hoeveelheden gegevens. De naam komt voort uit de overeenkomsten tussen het zoeken naar waardevolle bedrijfsinformatie en het graven (mining) naar iets waardevols in een grote berg (bron: Wikipedia).

136 Article 29 Data Protection Working Party, *Opinion nr. 4/2007 on the concept of personal data* WP 136 d.d. 20 november 2007 (http://ec.europa.eu/justice_home/fsj/ privacy/ docs/wpdocs/2007/wp136_nl.pdf)

gebruikers daarvan inbreuk op (haar) auteursrechten wordt gepleegd. Hierbij gaat deze houder ervan uit dat hij de internetgebruiker achter het IP adres zal kunnen identificeren, bijvoorbeeld door de relevante ISP te verzoeken de NAW-gegevens van de gebruiker te verstrekken, danwel in rechte verstrekking van deze gegevens te vorderen. Nu het IP adres wordt verwerkt om de gebruikers van de computer te identificeren, zal degene die de IP adressen verzamelt er kennelijk vanuit gaan dat "redelijkerwijs in te zetten middelen" aanwezig zijn om de persoon te identificeren, anders heeft die verwerking immers geen zin. De Art. 29 WG merkt hierbij wel op dat er voorbeelden denkbaar zijn waarbij identificatie met een IP adres nimmer mogelijk is, zoals in geval van een IP adres in een internetcafé waarbij voor gebruik geen identificatie wordt gevraagd[137]. Aangezien de ISP echter niet zal weten of een bepaald IP adres al dan niet identificeerbaar is, dient hij IP adressen volgens de Art. 29 WG schijnbaar voor alle zekerheid als persoonsgegevens te behandelen.

In 2008 heeft de Art. 29 WG zich weer uitgelaten over de verzameling van IP adressen op het internet[138]. In dit rapport spreekt de Art. 29 Werkgroep zich uitgebreid uit over de verwerking van persoonsgegevens door zoekmachines. Uit de door de Art. 29 WG bij diverse zoekmachines opgevraagde informatie blijkt dat bij elke zoekopdracht het IP adres wordt verzameld. Aan dit IP adres worden de zoekopdrachten gekoppeld, die met dat IP adres zijn uitgevoerd. In de ogen van de Art. 29 WG vindt hier daarom identificatie plaats.[139]

Volgens de Art. 29 WG wordt de mogelijkheid tot identificatie door middel van een (dynamisch) IP adres vergroot, als een cookie op de computer wordt geplaatst. Ook al wordt het dynamische IP adres iedere keer gewijzigd, zo stelt de Artikel

---

137 Ook is denkbaar dat een persoon zonder toestemming inlogt op een onbeveiligde Wifi-verbinding van een derde partij, waarbij niet snel traceerbaar zal zijn welke persoon op een gegeven moment gebruik maakte van een bepaald IP adres.

138 Article 29 Data Protection Working Party, *Opinion 1/2008 on data protection issues related to search engines*, WP 148 d.d. 4 April 2008 (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf)

139 Overigens kan in sommige gevallen ook met de enkele geschiedenis van met een bepaald IP adres uitgevoerde zoekopdrachten een bepaald persoon worden geïdentificeerd. Reden hiervoor is met name dat internetgebruikers de neiging hebben om informatie over zichzelf te zoeken. Maar ook zonder een dergelijke zoekopdracht is het soms mogelijk om door middel van het combineren van diverse zoekopdrachten van een persoon een bepaald – identificeerbaar – beeld van hem of haar te krijgen. Veelzeggend voorbeeld hiervan is het AOL search data scandal (http:// en.wikipedia.org/wiki/AOL_search_data_scandal). In de zomer van 2000 presenteerde AOL trots een bestand van 20 miljoen zoekopdrachten van 650.000 gebruikers. De diverse gebruikers werden enkel geïdentificeerd door een uniek nummer, waarmee hun anonimiteit zou moeten zijn gewaarborgd. Journalisten van de New York Times slaagden er niettemin in om diverse gebruikers te identificeren, waaronder een 62-jarige dame uit de Amerikaanse staat Georgia: Thelma Arnold.

29 Werkgroep, deze cookie blijft hetzelfde. Op deze wijze verzamelt de zoekmachine grote hoeveelheden gegevens over een bepaalde internetgebruiker, waardoor identificatie steeds beter zal kunnen plaatsvinden.

De Art. 29 WG gaat er ook in dit document vanuit dat een IP adres, ook al is het dynamisch, een persoonsgegeven in de zin van de Privacyrichtlijn is, schijnbaar mede op basis het hierboven genoemde cookie-argument. De Art. 29 WG maakt daarbij wel de kanttekening dat een zoekmachine zelf in de regel niet zal kunnen achterhalen wie de persoon achter een bepaald IP adres is. Deze gegevens zijn in beginsel enkel in handen van ISP's. De Art. 29 WG overweegt daarbij echter dat bepaalde autoriteiten – en in sommige landen ook private partijen door middel van civiele procedures – wel mogelijkheden hebben om identificerende gegevens van de ISPs te verkrijgen. Dit feit doet aan de mening van de Art. 29 WG dan ook niet af.

In haar werkdocumenten en opinies lijkt de Art. 29 WG ervan uit te gaan dat IP adressen vrijwel altijd herleidbaar zijn tot een natuurlijk persoon, en daarmee als persoonsgegeven moeten worden aangemerkt.[140] Zoals al eerder aangegeven wordt er hierbij aan voorbij gegaan dat een deel van de op het internet gebruikte IP adressen enkel aan computerhardware is toebedeeld (routers, servers), zonder dat daar een natuurlijke persoon aan te koppelen is.

De stellingen van de Art. 29 WG dat IP adressen altijd als persoonsgegevens moeten worden aangemerkt zouden derhalve nader moeten worden gekwalificeerd en beperkt: als een dergelijke stelling al zou kunnen worden ingenomen (naar de mening van de auteurs is dit niet, althans niet zonder voorwaarden, het geval) dan geldt dat enkel voor IP adressen die behoren bij direct door (eind) gebruikers gebruikte apparatuur en verbindingen.

Het College Bescherming Persoonsgegevens

De Nederlandse privacy waakhond, het CBP, neemt in de regel de mening van de Art. 29 WG over. Met betrekking tot het IP adres is het CBP zelfs wat stelliger dan de Art. 29 WG.

---

140 Deze conclusie leidt het CBP in ieder geval ook uit opinie 148 (Zoekmachines) van de Art. 29 WG af, zo blijkt uit haar persbericht over de publicatie van deze opinie (zie http://www.cbpweb.nl/documenten/pb_20080407_internet-zoekmachines.shtml): "*Naar de Opinie van de Artikel 29 Werkgroep is met spanning uitgezien. Het document biedt helderheid over definities – zo wordt ondubbelzinnig vastgesteld dat IP-adressen persoonsgegevens vormen – en het verschaft gebruikers en providers handvatten voor het vaststellen van hun rechten en plichten*."

De voorloper van het CBP, de Registratiekamer, oordeelde in maart 2001 dat een vast (statisch) persoonsgegeven te allen tijde als persoonsgegeven beschouwd diende te worden[141]. Zij redeneerde hierbij dat met behulp van de abonneeadministratie van de ISP de individuele gebruiker te herleiden is. Met betrekking tot het dynamische IP adres oordeelde de Registratiekamer dat dit alleen het geval was indien ook het moment van gebruik van het IP adres werd opgeslagen. Volgens de Registratiekamer kon alleen dan de ISP achterhalen op welk tijdstip zij het IP adres aan de desbetreffende abonnee had toegewezen.

Nadien hield het CBP zich lange tijd stil over de kwalificatie van het IP adres in termen van de Wbp. Wel deed zij in januari 2002 een interessante uitspraak over het criterium 'onevenredige inspanning', zoals dit in de hierboven geciteerde overweging 26 van de Privacyrichtlijn wordt verwoord in het kader van de identificeerbaarheid van de natuurlijke persoon[142]. Het CBP stelde daarbij dat identificeerbaarheid niet wordt aangenomen als hiervoor medewerking van derden buiten de macht en zeggenschap van de verantwoordelijke noodzakelijk is. Met dit criterium in de hand zou dit betekenen dat een IP adres voor iedereen behalve voor een ISP niet identificeerbaar en dus geen persoonsgegeven is[143]. Er is immers een derde, de ISP, voor nodig om de identiteit van de gebruiker te achterhalen. Voor deze kwalificatie valt veel te zeggen. Opmerkelijk is wel dat deze haaks staat op de hiervoor genoemde opinie van de Art. 29 WG. Later is het CBP daar in het kader van de kwalificatie van het IP adres als persoonsgegeven op teruggekomen, helaas zonder aan te geven wat voor haar aanleiding was om haar standpunt zo radicaal aan te passen.

In december 2007 heeft het CBP haar Richtsnoeren gepresenteerd met betrekking tot de publicatie van persoonsgegevens op het internet[144]. Hoewel deze Richtsnoeren (zoals de titel al doet vermoeden) zich met name richten op persoonsgegevens die op het internet zijn gepubliceerd, stelt en beantwoordt het CBP ook de vraag of een IP adres een persoonsgegeven in de zin van de Wbp is. Het CBP komt daarbij tot een volmondig ja. Dit omdat volgens het CBP een IP adres door een derde – de ISP – eenvoudig te herleiden valt tot een natuurlijk persoon (de afnemer

141 College Bescherming Persoonsgegevens, "*Een IP adres is niet altijd een persoonsgegeven*", 19 maart 2001, z2000-0340 (http://www.cbpweb.nl/downloads_uit/z2000-0340.pdf).

142 College Bescherming Persoonsgegevens, "*Mag het een bitje minder zijn? Over Privacy-Enhancing Technologies*" januari 2002 (http://www.cbpweb.nl/downloads_brochures/Bro_PET.pdf)

143 Tot deze conclusie komen ook R. van Esch & P. Blok, 'Privacy en elektronische handel op het internet' in (J.M.A. Berkvens & prof.mr. J.E.J. Prins red.) *Privacyregulering in theorie en praktijk* Kluwer, Deventer, 2007, p. 206.

144 CBP Richtsnoeren, *Publicatie van Persoonsgegevens op het Internet*, 11 December 2007 (http://www.cbpweb.nl/downloads_rs/rs_20071211_persoonsgegevens_op_internet_definitief.pdf)

van het internetabonnement). Het CBP concludeert hier gemakshalve dat dit ook geldt voor dynamische IP adressen die worden verwerkt in combinatie met datum en tijd. Het maakt daarbij volgens het CBP niet uit of de ISP met het IP adres ook daadwerkelijk een persoonsgegeven zal gaan identificeren; het enkele feit dat deze mogelijkheid bestaat is al voldoende. Ten slotte is volgens het CBP

> *"van belang dat op basis van het IP adres beslissingen kunnen worden genomen over de toegang tot bepaalde informatie, zonder dat een dienstverlener op het internet überhaupt enige moeite hoeft te doen om zelf persoonsgegevens te verbinden aan een IP adres".*

4.4 Enkele kanttekeningen

4.4.1 Consistentie

Zowel het CBP als de Art. 29 WG stellen zich (thans) op het standpunt dat een IP adres (vrijwel) altijd als een persoonsgegeven aangemerkt moet worden. Dit is een verregaande conclusie, waarbij beide instanties terecht ook zelf kanttekeningen plaatsen:

> *"in sommige gevallen is het voor bepaalde IP adressen om technische en organisatorische redenen niet mogelijk de gebruiker daarvan te identificeren"*[145]
>
> *en*
>
> *"niet-identificeerbaarheid (wordt) aangenomen als hiervoor de medewerking van derden buiten de macht en zeggenschap van de verantwoordelijke noodzakelijk is"*[146].

Het is dus, ook volgens het CBP en de Art. 29 WG, duidelijk dat voor vele verwerkers van IP adressen, de ISP's daargelaten, geen redelijkerwijs in te zetten middelen bestaan om een IP adres te herleiden tot een bepaald persoon. Voor een gemiddelde verwerker zal deze herleiding pas mogelijk zijn nadat een verzoek aan een ISP om verstrekking van persoonsgegevens van een gebruiker wordt gehonoreerd**.** Het ontbreken van de mogelijkheid om het IP adres te herleiden tot een bepaald persoon zou ons inziens tot de conclusie leiden dat een IP adres in een dergelijke situatie geen persoonsgegeven is.

---

145 Zie voetnoot 139 (Artikel 29 Werkgroep, april 2007 (WP 136))

146 Zie voetnoot 145 (College Bescherming Persoonsgegevens, januari 2002)

Opmerkelijk is dat het CBP in het kader van de kwalificatie van het IP adres volledig voorbij gaat aan haar hierboven genoemde eerdere standpunt[147] dat een bepaald gegeven geen persoonsgegeven is indien een derde buiten de macht en zeggenschap van de verantwoordelijke nodig is om het gegeven naar een bepaald persoon te herleiden. Interessant is verder dat het CBP haar redenering ondersteunt door te stellen dat op basis van het IP adres "beslissingen" kunnen worden genomen zonder dat de dienstverlener moeite heeft moeten doen om de identiteit van de internetgebruiker te achterhalen, zonder dat wordt onderbouwd waar het criterium van het nemen van "beslissingen" op is gestoeld.

De Art. 29 WG is geen toezichthoudende autoriteit en kan op grond van artikel 30 van de Privacyrichtlijn alleen adviezen geven en aanbevelingen doen. Deze worden doorgaans normaliter als gezaghebbend, maar worden in de rechtspraak lang niet altijd gevolgd. Dat blijkt bijvoorbeeld uit twee uitspraken van het Franse Hof van Beroep uit 2007 die handelden over de identificeerbaarheid van IP adressen. In een eerste uitspraak oordeelde dit Hof dat een IP adres geen persoonsgegeven is omdat het enkel verbonden is aan een bepaald apparaat en enkel de opsporingsautoriteiten kunnen achterhalen wie gebruik maakt van dat apparaat[148]. In de tweede uitspraak oordeelde het Hof dat een IP adres alleen aan een apparaat is verbonden en niet aan degene die een bericht op het internet achterlaat[149].

Ook in Duitsland bestaat onenigheid en dus onduidelijkheid of een IP adres dient te worden aangemerkt als een persoonsgegeven. In een uitspraak van het Ambtsgericht te Berlijn[150] werd de opinie van de Art. 29 WG gevolgd. Geoordeeld werd dat een IP adres als een persoonsgegeven diende te worden aangemerkt, aangezien:

> *"es durch die Zusammenführung der personenbezogenen Daten mit Hilfe Dritter bereits jetzt ohne großen Aufwand in den meisten Fällen möglich [ist], Internetnutzer aufgrund ihrer IP-Adresse zu identifizieren."*

Deze uitspraak is bevestigd in Hoger Beroep door het Landgericht in Berlijn[151].

---

147 Zie voetnoot 145 (College Bescherming Persoonsgegevens, januari 2002)

148 Cour d'appel de Paris, 13eme chambre section B Arret du 27 avril 2007, Anthony G. / SCPP (http://www.legalis.net/jurisprudence-decision.php3?id_article=1954)

149 Cour d'appel de Paris, 13eme chambre section A Arret du 15 may 2007, Henri S. / SCPP (http://www.legalis.net/jurisprudence-decision.php3?id_article=1955)

150 Ambtsgericht Berlin-Mitte, Geschäftsnummer: 5 C 314/06, 27.03.2007

151 Landsgericht Berlin, Geschäftsnummer: 23 S 3/07, 06.09.2007

Het Ambtsgericht van München heeft op 30 september 2008 echter anders geoordeeld. In deze zaak overwoog de rechter dat een IP adres geen persoonsgegeven is, aangezien alleen een *access provider* het IP adres kan gebruiken om de persoon die daarvan gebruik maakt, te identificeren[152].

De Engelse toezichthouder, de Information Commissioner's Office ("ICO") worstelt in haar richtlijn inzake het verzamelen van persoonsgegevens via het internet (*Good practice note – Collecting personal information using websites, 5 juni 2007*[153]) ook met de kwalificatie van een IP adres als persoonsgegeven. In theorie, zo stelt zij, dient, een IP adres te worden aangemerkt als een persoonsgegeven. De ICO is echter reëel, en stelt dat het in de praktijk lastig zal zijn om met een IP adres een persoon te identificeren. Hierover schrijft de ICO het volgende:

> *"In practice, it is difficult to use IP addresses to build up personalised profiles. Many IP addresses, particularly those allocated to individuals, are 'dynamic'. This means that each time a user connects to their internet service provider (ISP), they are given an IP address, and this will be different each time. So if it is only the ISP who can link the IP address to an individual it is difficult to see how the Act [bedoeld is de UK Data Protection Act 1998, red.] can cover collecting dynamic IP addresses without any other identifying or distinguishing information".*

Onduidelijk is waarom zowel het CBP als de Art. 29 WG de Franse rechtspraak en de richtlijn van de Engelse toezichthouder niet in hun analyses hebben betrokken (en andersom, waarom in bovengenoemde rechtspraak en richtlijn niet altijd de opinie van de Art. 29 WG is meegenomen). Van echte harmonisatie van de uitleg van de Europese privacy-regelgeving op dit gebied blijkt derhalve nog geen sprake te zijn. Voor wat betreft het CBP werpt dit tevens de vraag op waarom zij ervoor heeft gekozen om zonder enige toelichting terug te komen op haar eerdere standpunt over identificeerbaarheid. De indruk bestaat daardoor dat men er gewoon niet aan wil dat IP adressen soms toch niet als persoonsgegevens kunnen kwalificeren.

4.4.2 Implicaties

Als IP adressen altijd kwalificeren als persoonsgegevens – wat zoals gezegd door zowel het CBP als de Art. 29 WG wordt betoogd – dan betekent dat dat de Wbp

152 Ambtsgericht München, Geschäftsnummer: 133 C 5677/08, 30.09.2008

153 http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/collecting_personal_information_from_websites_v1.0.pdf

in heel veel gevallen van toepassing is op de verwerking van deze gegevens. De implicaties daarvan zijn verstrekkend. Een integrale bespreking van alle implicaties gaat op deze plaats te ver. Volstaan wordt daarom met het kort signaleren van enkele ervan:

Informatieplicht
Als IP adressen persoonsgegevens zijn moet degene die door deze gegevens wordt geïdentificeerd – gemakshalve gaan wij er maar even vanuit dat dit de internetgebruiker is – op grond van artikel 33 en 34 Wbp worden geïnformeerd over de identiteit van de verantwoordelijke, over de doeleinden waarvoor de gegevens worden verwerkt en verder alles wat nog nodig is om een behoorlijke en zorgvuldige verwerking te waarborgen. En dat moet gebeuren ofwel op het moment dat de gegevens worden vastgelegd ofwel op het moment dat de gegevens aan een derde worden verstrekt. Deze verplichting geldt niet voor zover de betrokkene al op de hoogte is van de desbetreffende gegevensverwerking.

Naar onze mening zal de gemiddeld geïnformeerde internetgebruiker niet op de hoogte, althans zich er niet van bewust, zijn dat het IP adres van zijn computer door een website aanbieder wordt verwerkt. Dit houdt in dat iedere website aanbieder zijn bezoekers moet informeren over deze verwerking en het doel daarvan en de daarbij gebruikte middelen. Dergelijke informatie kan bijvoorbeeld in algemene voorwaarden of in een privacybeleid van een website worden opgenomen.
ISP's zullen in het kader van de eigen dienstverlening, te weten het verschaffen van toegang tot het internet, IP adressen vastleggen. Over deze verwerking zullen de ISP's degenen die de dienst afnemen moeten informeren (wij gaan er ook hierbij vanuit dat de gemiddeld geïnformeerde internetgebruiker zich er niet altijd van bewust is dat zijn IP adres door de ISP wordt verwerkt). Met de redenering van de Art. 29 WG en het CBP ten aanzien van de kwalificatie van het IP adres als persoonsgegeven in het achterhoofd kan men zich afvragen of deze informatieplicht wellicht verder gaat. Dient een ISP al haar gebruikers te informeren dat hun IP adres – al dan niet op vordering van de rechter – kan worden gebruikt om hen als persoon achter bepaalde door middel van het desbetreffende IP adres uitgevoerde handelingen op het internet kan identificeren? Of geldt deze verplichting alleen op het moment dat een dergelijke situatie zich voordoet?

Meldplicht
Op grond van artikel 27 Wbp moeten verwerkingen van persoonsgegevens worden aangemeld bij het CBP. Verwerkingen die veel voorkomen, standaard zijn en die geen grote risico's meebrengen zijn vrijgesteld van deze meldingsplicht op

grond van het Vrijstellingsbesluit. Voorbeelden hiervan zijn bijvoorbeeld standaard verwerkingen in het kader van een personeels- of klantenadministratie of bestanden die worden gebruikt voor communicatie van direct marketing. Er gelden op dit moment nog geen vrijstellingen voor het verwerken van persoonsgegevens die zijn verzameld via het internet. Wellicht dat sommige verwerkingen van IP adressen onder vrijstellingen voor klanten- of communicatiebestanden zullen vallen. In alle andere gevallen zal de websitehouder (de verantwoordelijke in de zin van de Wbp) de verzameling van IP adressen aan het CBP moeten melden[154].

Recht op inzage
Een betrokkene heeft recht op toegang tot de persoonsgegevens die van hem zijn verzameld, aldus artikel 35 Wbp. De aanname dat een IP adres een persoonsgegeven is, houdt dus in dat een internetgebruiker het recht heeft op inzage in de IP adressen die van hem zijn verzameld. Een gemiddelde websitehouder zal aan dit verzoek echter niet kunnen voldoen; hij weet immers niet welk IP adres bij de verzoeker hoort. Dit zal de betrokkene dan ook zelf moeten verstrekken, of de websitehouder zal contact moeten zoeken met de ISP van de internetgebruiker. Op dit punt is de Wbp – als de redenering in acht wordt gehouden dat een IP adres te allen tijde een persoonsgegeven is – dan ook niet uitvoerbaar.

4.5 Wie bepaalt wat gebeurt met verkeers- en locatiegegevens?

4.5.1 Inleiding

Voor verkeers- en locatiegegevens, of telecommunicatiegebruiksgegevens, heeft de gemeenschapswetgever gemeend veel strengere regels te moeten vaststellen dan voor de meeste gewone persoonsgegevens. Dat heeft hij gedaan in de Richtlijn privacy en elektronische communicatie 2002/58/EG (de zgn. ‘e-privacyrichtlijn’) en later in de zogeheten Data Retentie Richtlijn 2006/24/EG, die een enkel onderdeel van de eerste richtlijn aanpast. De beide richtlijnen zijn in het nationale recht geïmplementeerd door artikel 11.5 en 11.5a Tw.

154 Het lijkt erop dat dit op dit moment niet gebeurt; zoals wel vaker heeft het CBP nog geen reden gezien of capaciteit gehad om deze mogelijke overtreding van de Wbp te bestraffen.

De reden waarom de gemeenschapswetgever voor deze categorie van gegevens strengere regels heeft vastgesteld, wordt uiteengezet in de preambule bij de e-privacyrichtlijn, zij het niet heel duidelijk. De e-privacyrichtlijn geeft aan dat er in de context van telecommunicatie of elektronische communicatie nieuwe geavanceerde digitale technologieën worden ingevoerd die met betrekking tot de bescherming van de persoonsgegevens en de persoonlijke levenssfeer van de gebruiker 'specifieke eisen' stellen. Ook geeft de preambule aan dat van dergelijke technologieën gebruik wordt gemaakt om allerlei nieuwe, vaste en mobiele netwerken op te tuigen. En in deze netwerken ontstaan veel nieuwe mogelijkheden om steeds meer gegevens, waaronder persoonsgegevens, te verwerken. Het succes van deze netwerken en de daarmee aangeboden diensten wordt mede bepaald door het vertrouwen van de gebruikers dat hun persoonlijke levenssfeer zal worden geëerbiedigd. Om te komen tot een succesvolle ontwikkeling van dergelijke nieuwe diensten acht de gemeenschapswetgever het nodig om te voorzien in extra waarborgen voor het gebruik van dergelijke, via deze nieuwe diensten verwerkte gegevens.[155]

4.5.2 Wat zijn verkeers- en locatiegegevens?

Waar het gaat om verkeers- en locatiegegevens gaat de e-privacyrichtlijn, en dus ook de wet die deze implementeert, uit van de volgende begripsomschrijvingen:

- onder ***verkeersgegevens*** verstaat artikel 11.1, onder b, van de Telecommunicatiewet (Tw) de gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan.
- de ***verwerking*** van deze verkeersgegevens wordt aangemerkt als een verwerking van persoonsgegevens, zoals bedoeld in artikel 1, onderdeel b, Wbp, met dien verstande dat de desbetreffende verwerkingshandelingen mede betrekking hebben op verkeersgegevens van abonnees die geen natuurlijke personen zijn.
- onder ***locatiegegevens*** worden in artikel 11.1, onder d, Tw de gegevens verstaan die worden verwerkt in een elektronisch communicatienetwerk waarmee de geografische positie van de randapparatuur van een gebruiker van een openbare elektronische communicatiedienst wordt aangegeven.

Van belang daarbij is dat een abonnee in artikel 1.1, onder p, Tw wordt opgevat als de natuurlijke persoon of rechtspersoon die partij is bij een overeenkomst met

155 Aldus overw. 5 en 6 van de preambule bij de e-privacyrichtlijn

een aanbieder van openbare elektronische communicatiediensten voor de levering van dergelijke diensten. Dat kan dus een individu zijn die voor zichzelf een abonnement is aangegaan. Maar het zou ook een werkgever kunnen zijn die ten behoeve van zijn werknemers een abonnement is aangegaan. In het laatste geval is de abonnee niet ook gebruiker, want dat begrip wordt in artikel 11.1, onder a, Tw[156] gedefinieerd als een natuurlijke persoon die gebruik maakt van een openbare elektronische communicatiedienst voor particuliere of zakelijke doeleinden zonder noodzakelijkerwijze op die dienst te zijn geabonneerd.

4.5.3 Wat mag (niet) met verkeers- en locatiegegevens?

Voor de verschillende categorieën van gegevens worden regels gegeven in verschillende wetten, die uitvoering geven aan de privacyrichtlijn 95/46/EG en de e-privacyrichtlijn 2002/58/EG, en omdat de begripsomschrijvingen van persoonsgegevens, verkeersgegevens en locatiegegevens elkaar gedeeltelijk overlappen, moet er rekening mee worden gehouden dat deze regels in voorkomende gevallen cumulatief gelden.

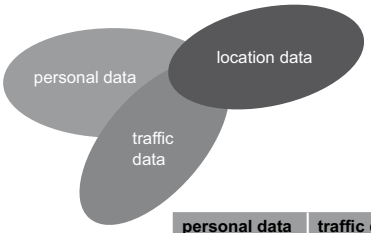
- ***persoonsgegevens*** hebben altijd betrekking op individuele natuurlijke personen en als zodanig geeft de privacyrichtlijn 95/46/EG cq. de Wbp daarvoor de regels;
- ***verkeersgegevens*** betreffen de wijze waarop individuele natuurlijke personen en/of rechtspersonen gebruik maken van elektronisch communicatienetwerk; de regels voor deze gegevens staan in de e-privacy-richtlijn en de Telecommunicatiewet en soms, als het tegelijkertijd persoonsgegevens betreft, ook in de Wbp;
- ***locatiegegevens*** betreffen gegevens over de locatie van apparatuur van een individuele natuurlijke persoon in een elektronisch communicatienetwerk; de regels voor deze gegevens staan in de e-privacyrichtlijn en de Telecommunicatiewet en omdat het tegelijkertijd vaak (altijd?)[157] persoonsgegevens betreft, ook in de Wbp.

---

156 In afwijking van art. 1.1, onder n, Tw!

157 Uit de verschillende definities zou kunnen worden opgemaakt dat locatiegegevens altijd betrekking hebben op (randapparatuur van) een gebruiker, zijnde een natuurlijke persoon. Echter, het is voorstelbaar dat de gebruiker zich niet altijd dezelfde locatie bevindt als zijn randapparatuur, en ook dat de gebruiker niet altijd kan worden vereenzelvigd met de abonnee. Het is daarom misschien niet *persé* uitgesloten dat de locatiegegevens niet direct betrekking hebben op een natuurlijke persoon, en wel op een rechtspersoon. Toegegeven: vergezocht is dat wel.

Schematisch zou een en ander zo kunnen worden weergegeven:



	personal data	traffic data	location data
about whom?	natural person	natural persons and legal entities	natural persons and lega entities
about what?	all aspects	use of electronic network	geographic position equipment
Directive	95/46/EC	02/58/EC 06/24/EC	02/58/EC 06/24/EC

De regels voor persoonsgegevens staan in de Wbp en zijn in het voorgaande kort besproken. Zoals gezegd staan de regels voor verkeers- en locatiegegevens in de Telecommunicatiewet, en wel in artikel 11.5 en artikel 11.5a Tw.

Artikel 11.5 Tw heeft betrekking op verkeersgegevens, waaronder mede begrepen locatiegegevens die ook verkeersgegevens zijn. Het gaat om gegevens over de communicatie, maar niet de communicatie zelf. Dus niet uw telefoongesprek of de inhoud van uw e-mailbericht, maar het moment waarop u heeft gebeld en hoelang dat gesprek heeft geduurd, de omvang van uw e-mailbericht en of er al dan niet attachments aan waren verbonden, de locatie waar u zich bevond toen met uw mobiele telefoontoestel werd gebeld, de IMSI- en EIMI-nummers van dat mobiele telefoontoestel, en dergelijke.

Deze en allerlei andere verkeersgegevens moeten door de aanbieder van de elektronische communicatiedienst worden vernietigd of geanonimiseerd, zodra deze niet langer nodig zijn ten behoeve van de overbrenging van communicatie of de facturering daarvan. Onder het overbrengen van de communicatie en de facturering daarvan wordt ook verkeersbeheer begrepen, alsmede de behandeling van verzoeken om inlichtingen van klanten, de opsporing van fraude en de beslechting van geschillen. De wet laat er daarbij geen misverstand over bestaan dat de gegevens mogen worden bewaard en verwerkt tot het einde van de wettelijke termijn waarbinnen de factuur in rechte kan worden betwist of de betaling in rechte kan worden afgedwongen. Als de algemene voorwaarden zouden voorschrijven

dat de abonnee een factuur binnen drie maanden moet betwisten, dan kunnen de verkeersgegevens ook niet langer dan die drie maanden worden bewaard.

In aanvulling daarop mogen deze gegevens worden gebruikt voor marktonderzoek of verkoopactiviteiten met betrekking tot elektronische communicatiediensten, én de levering van diensten met toegevoegde waarde. Echter, alleen als de abonnee of de gebruiker daarvoor zijn toestemming heeft gegeven. De abonnee of gebruiker kan de gegeven toestemming voor de verwerking van verkeersgegevens te allen tijde intrekken.

Verder is van belang dat deze gegevens alleen mogen worden verwerkt door personen die werkzaam zijn onder het gezag van de aanbieder. De aanbieder moet dus te allen tijde controle en zeggenschap houden over de verwerking. En als hij de verwerking zou willen uitbesteden, dan kan dat alleen als hij het gezag over de desbetreffende personen heeft.

Een en ander is aanmerkelijk strenger dan wat de Wbp toestaat. Een aanbieder die de gegevens wil gebruiken om andere dan elektronische communicatiediensten te verkopen, mag dat niet– zelfs niet als de abonnee daarover goed is geïnformeerd en vervolgens ondubbelzinnige toestemming heeft gegeven. De wetgever laat de abonnee niet de vrijheid om daarover zelf te beslissen. Waarom de wetgever wat dit betreft zo weinig vertrouwen heeft in de abonnees, is niet duidelijk. En dat is, zacht gezegd, merkwaardig.[158]

Voor locatiegegevens die niet ook verkeersgegevens zijn geeft artikel 11.5a Tw nog enige regels. Voor deze gegevens moet vooral worden gedacht aan GPS-gegevens die in de wat modernere randapparaten worden gebruikt om de locatie daarvan te bepalen. Het gaat dus niet om de gegevens die in het elektronisch communicatienetwerk worden gebruikt om de gesprekken naar de juiste netwerkcel te routeren, maar om extra locatiebepalingsfaciliteiten, zoals de navigatiemogelijkheden die in sommige pda's zijn ingebouwd (Blackberrry met GPS, smartphone met TomTom).

158 Vgl. G-J. Zwenne 'Verkeersgegevens in de Telecommunicatiewet en de Wet bescherming persoonsgegevens' *Mediaforum* 2000/5, pp. 152-157; G-J. Zwenne, 'Verkeersgegevens en persoonsgegevens in de Telecommunicatiewet en de Wet bescherming persoonsgegevens: de toegevoegde waarde van specifieke privacyregelgeving', in: P.B. Cliteur, H.J. van den Herik, N.J.H. Huls & A.H.J. Schmidt (Eds.), '*It ain't necessarily so'*, in: Meijers-reeks, nr. 38, pp. 533-546. Deventer: Kluwer (2001).

Deze gegevens mogen, zo blijkt uit artikel 11.5a Tw, alleen worden verwerkt als de gegevens zijn geanonimiseerd of, met toestemming van de abonnee of gebruikers, ten behoeve van de levering van een dienst met toegevoegde waarde, zoals locatiegebonden diensten. Als er zo een toegevoegde waardedienst wordt geleverd mogen de gegevens, uiteraard, ook worden gebruikt voor de facturering van die dienst. Ook deze gegevens mogen alleen worden verwerkt door personen die werkzaam zijn onder het gezag van de aanbieder van de elektronische communicatiedienst, dan wel de aanbieder van de toegevoegde waardedienst.

4.5.4 De bewaarplicht verkeers- en locatiegegevens

In de data retentierichtlijn 2006/24/EG verlangt de gemeenschapswetgever dat de lidstaten ervoor zorgdragen dat een aantal categorieën van verkeers- en locatiegegevens door de aanbieders van elektronische communicatiediensten en -netwerken gedurende minimaal 6 en maximaal 24 maanden worden bewaard, ten behoeve van het onderzoek naar en de opsporing en vervolging van ernstige criminaliteit. De wetgever wil zo bereiken dat politie, justitie en inlichtingendiensten, zonodig, over deze gegevens kunnen beschikken.

In Nederland is, evenals eerder in het Europees Parlement, veel en uitvoerig gediscussieerd over deze bewaarplicht.[159] Daarbij ging het overwegend over de bewaartermijn. In het wetsvoorstel dat naar de kamer is gestuurd zette de regering in op 18 maanden, vanuit de kamer werd vrijwel direct aangedrongen op 6 maanden. De uitkomst van dit onderhandelingsproces is, thans,[160] 12 maanden, waarmee Nederland zich voegt bij de meerderheid van de lidstaten.[161]

4.6 Afsluitende opmerkingen

Als het gaat om vragen over wie er controle heeft over internet, internetgebruik en internetgebruikers kan niet voorbij worden gegaan aan wie wat mag met IP

---

159 Zie daarover G-J. Zwenne & A.H.J. Schmidt, 'Opmerkingen bij het wetsvoorstel Wet bewaarplicht telecommunicatiegegevens', *Mediaforum* 2008/7-8, p. 278-285, alsmede A.H.J. Schmidt & G-J. Zwenne, 'Recht & Risico: Kanttekeningen bij het voorstel voor een richtlijn over de bewaring van telecommunicatie verkeersgegevens', *Mediaforum* 2005/9, p. 292-302.

160 Het gewijzigd voorstel van wet (Wet Bewaarplicht Telecommunicatiegegevens, Kamerstuk 2007-2008, 31145, nr. A, Eerste Kamer) is op 26 mei 2008 naar de Eerste Kamer gestuurd.

161 Vgl. www.twobirds.com/english/publications/articles/Implementation_Data_Retention_Directive_0208.cfm

adressen en verkeers- en locatiegegevens. Een regeling daarvoor staat, voor een belangrijk deel, in achtereenvolgens de Wbp en de Tw.

Wat betreft IP adressen is gebleken dat de nationale privacytoezichthouder, in aansluiting op wat de Art. 29 WG zegt, zich zonder al te veel voorbehouden op het standpunt stelt dat deze gegevens haast vanzelfsprekend moeten worden aangemerkt als persoonsgegevens. En dat betekent dat de Wbp altijd van toepassing is op de verwerkingen van deze gegevens, zelfs indien dat onuitvoerbare verplichtingen oplevert (§ 2.4.2c).

Daar valt het nodige op af te dingen, en niet alleen omdat het CBP daarmee opzichtig voorbijgaat aan eerder door haar ingenomen standpunten. Vaststaat dat IP adressen heel wel persoonsgegevens kunnen zijn. Maar ook heel wel niet. Het hangt er maar vanaf wie of wat wordt geïdentificeerd door het IP adres. Als IP adressen op dit moment al niet veelal apparaten en dus geen gebruikers identificeren, dan is dat zeker in de toekomst het geval. Als IP6 wordt ingevoerd en het aantal mogelijke IP adressen exponentieel toeneemt, zal het eerder regel dan uitzondering zijn dat deze gegevens niet (meer) als persoonsgegevens kunnen worden aangemerkt.

Wat verkeers- en locatiegegevens betreft is sprake van een verontrustende trend. De nieuwe wettelijke bewaarplichten brengen mee dat zeggenschap en controle over de gegevens steeds meer komt te liggen bij politie, justitie en inlichtingendiensten.