Prof.mr. Gerrit-Jan Zwenne

De verwaterde privacywet

Universiteit Leiden

De verwaterde privacywet

Oratie uitgesproken door

prof.mr. Gerrit-Jan Zwenne

bij de aanvaarding van het ambt van hoogleraar
Recht en de Informatiemaatschappij
aan de Universiteit Leiden
op vrijdag 12 april 2013

Universiteit
Leiden

Inhoud

Mijnheer de rector-magnificus, zeer gewaardeerde toehoorders,

Wie geeft er nog om privacy?

"Wie geeft er nog om privacy?". Dat vroeg Frank Kuitenbrouwer zich af in de NRC van 15 september 2007.[1] De aanleiding voor deze verzuchting was een opinietekst, waarin twee jonge onderzoekers van deze universiteit het hadden bestaan te zeggen dat de privacywetgever te ambitieus is, dat de werkingssfeer van de privacywet te onbepaald is en dat de regels ervan soms onbegrijpelijk zijn.[2]

"Je moet wél durven", zei Kuitenbrouwer daarover, "om de privaywet 'te ambitieus' te noemen. Kan dat ooit gelden voor burgerlijke vrijheden?"

Deze vraag is ook nu nog actueel. Op dit moment wordt in Brussel een nieuwe privacywet[3] voorbereid. In dat verband wordt voorgesteld de werkingssfeer van die wet op te rekken. De huidige privacywet is van toepassing op gegevens over personen waarvan de identiteit bekend is of bekend kan worden. Voorgesteld wordt dat de wet voortaan ook van toepassing moet zijn op de gegevens waarmee de éne persoon van de ander kan worden onderscheiden, zonder dat de identiteit daarvan bekend is.

Een dergelijk voorstel is ambitieus. En, inderdaad, misschien wel *te* ambitieus. Als de privacywet geldt voor alle gegevens waarmee de éne persoon van de andere kan worden onderscheiden, kunnen we ons geen goede voorstelling meer maken van de situaties waarin de wet *niet* van toepassing is. De maatstaf voor de toepassing ('het-kunnen-onderscheiden-van-anderen') heeft zo weinig onderscheidend vermogen, dat de werkingssfeer van de wet zowat onbegrensd wordt. Je zou dat kunnen duiden als verwatering van de privacywet.

Is dit erg? Het gaat toch om burgerlijke vrijheden? Ja. Dat is erg, juist omdat het gaat om burgerlijke vrijheden. We moeten dan werkingssfeer van de wet op de een of andere manier weer gaan inperken, met als gevolg veel rechtsonzekerheid. En daardoor wordt de privacywet nog veel lastiger dan die nu al is.

Vanmiddag ga ik in op de werkingssfeer van de privacywet. Ik doe dat aan de hand van de vraag of die wet van toepassing is, of zou moeten zijn, op IP-adressen. Deze vraag, en de verschillende antwoorden die daarop de afgelopen jaren zijn gegeven, bieden inzicht in de ambities van de privacywetgever en de rol van privacytoezichthouders. En dat is waarover ik het vandaag met u wil hebben.

Ik begin met een kort hoorcollege over wat persoonsgegevens zijn.

Een kort hoorcollege over persoonsgegevens

De privacywet is van toepassing op persoonsgegevens.
Een persoonsgegeven is 'iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon', aldus de definitie uit de Europese privacyrichtlijn.[4] En daarbij wordt onder 'identificeerbaar' verstaan,
(ik citeer):

> "*een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of [aan de hand] van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit*"

(einde citaat).

Hieruit kan níet goed worden opgemaakt *wat* de wetgever precies bedoelt met 'identificeren'. Wél *hoe* er kan worden geïdentificeerd. Dat kan aan de hand van een nummer of aan de hand van specifieke kenmerken van iemands identiteit. Het gaat erom dat de degene die over de gegevens beschikt (we noemen die wel 'de verantwoordelijke'), of iemand anders, met de hem beschikbare middelen redelijkerwijs de identiteit van de desbetreffende persoon kan achterhalen.

Uit de overwegingen bij de privacyrichtlijn[5] en de parlementaire geschiedenis van de privacywet[6] en uit de literatuur daarover,[7] destilleer ik drie aspecten die daarbij van belang zijn.

Ik neem ze met u door.

1. Identiteit. In de eerste plaats gaat het om de identiteit van degene op wie de gegevens betrekking hebben (we noemen die wel 'de betrokkene'). Er is sprake van persoonsgegevens als het mogelijk is om de identiteit van die betrokkene te achterhalen. Een gegeven is nog géén persoonsgegeven omdat het iets zegt over iemand, en zelfs niet omdat het uniek is voor iemand, maar omdat het betrekking heeft op iemand waarvan de identiteit bekend is of kan worden.

Een telefoonnummer, een kenteken of een vingerafdruk, het zijn op zichzelf nog geen persoonsgegevens. Maar ze zijn dat mogelijk wel in combinatie met andere gegevens, zoals de naam- en adresgegevens in het telefoonboek, de gegevens in het kentekenregister of in een vingerafdrukken-databank. Want, behoudens de gevallen waarin het gaat om spontane herkenning, maakt de combinatie van deze gegevens het mogelijk om iemand te identificeren.[8]

Ik noem dat het identiteitsaspect.

2. Redelijkheid. In de tweede plaats is er het redelijkheidsaspect. Er is alleen sprake van persoonsgegevens als het geen onevenredige inspanning kost om de identiteit van de betrokkene te achterhalen. Als het achterhalen van de identiteit, gegeven de redelijkerwijs beschikbare identificatiemogelijkheden, een onevenredige inspanning vergt, is er geen sprake van identificeerbaarheid. En evenmin van persoonsgegevens.

Een theoretische identificatiemogelijkheid is dus onvoldoende is om te kunnen spreken van persoonsgegevens.[9] Het moet wel 'te doen' zijn.

3. Relativiteit. In de derde plaats is er het relativiteitsaspect. Een gegeven kan ten opzichte van de éne persoon worden aangemerkt als persoonsgegeven en tegelijkertijd tegenover een andere persoon niet. Daarvan is sprake als die éne persoon wel, en de andere niet, over de mogelijkheden beschikt om achter de identiteit van de betrokkene te komen.[10]

Het relativiteitsaspect houdt verband met het redelijkheidsaspect. Wat voor de één wél in redelijkheid is te doen, is dat niet voor de andere. En daarom is het, gelet op de bescherming van de betrokkenen, redelijk om van die éne wél, en van de andere niet, te verlangen dat de gegevens worden behandeld als persoonsgegevens.

> Een voorbeeld om een en ander verduidelijken. Ik heb hier een glas en daarop staat een vingerafdruk. U kunt die niet zien. Ik wel. Die vingerafdruk is niet van mij. Ik heb het glas niet aangeraakt, houd het vast met een tissue. En we weten dus niet van wie de vingerafdruk is. En daarom is deze vingerafdruk, hoewel zonder meer uniek voor een bepaalde persoon, toch geen persoonsgegeven. Dat is waar het identiteitsaspect op ziet.
>
> Er kan met die vingerafdruk misschien wel iemand worden geïdentificeerd. Bijvoorbeeld met behulp van een vingerafdrukkendatabank. Maar dat gaat u en mij niet lukken. Wij hebben geen toegang tot die databank. Het is voor ons daarom een onredelijke inspanning om de identiteit van die persoon te achterhalen. Vanwege het redelijkheidsaspect hoeven wij daarom dit glas, en de vingerafdruk daarop, niet als persoonsgegeven te behandelen. En dat is maar goed ook. Het zou de afwas anders onnodig kunnen compliceren.
>
> Dat kan allemaal anders zijn voor de het Nationaal Forensisch Instituut. Want daar heeft men, vermoed ik, toegang tot een vingerafdrukkendatabank. En daar kan men dan zonder onevenredige inspanning achterhalen van wie de vingerafdruk is. En in dat geval

is de vingerafdruk wel een persoonsgegeven. Maar alleen voor het instituut, níet voor ons. Dat is waar het relativiteitsaspect op ziet.

De drie aspecten maken het persoonsgegevensbegrip contextafhankelijk en dynamisch. Wat op enig moment, in een bepaalde context, voor de één heeft te gelden als persoonsgegeven, kan heel wel op een ander moment of voor een ander géén persoonsgegeven zijn. De drie aspecten maken dat de privacywet van toepassing is waar dat nodig is, en níet waar dat niet nodig is. Ze maken de wet werkbaar en geven eraan betekenis, en ze dragen zo dragen bij aan de effectiviteit ervan. Wat dat betreft zijn deze drie aspecten essentieel voor de werking van de privacywet.

Maar tegelijkertijd maken deze aspecten het persoonsgegevensbegrip lastig. Ze maken dat de vraag of er sprake is van persoonsgegevens, vaak niet gemakkelijk te beantwoorden is. Het hangt er vanaf. En dat is altijd lastig.

Tot zover mijn korte hoorcollege over wat persoonsgegevens zijn. Ik ga verder met de vraag of IP-adressen als zodanig moeten worden aangemerkt.

Zijn IP-adressen wél of géén persoonsgegevens?
IP-adressen zijn de nummers die worden toegekend aan internetaanbieders, die deze weer toewijzen aan de computers, tablets en smartphones van hun abonnees. IP-adressen maken dat deze apparaten vindbaar zijn op het internet.[11]

Zijn IP-adressen nu wél of géén persoonsgegevens? Vaak wel. En vaak niet. Het hangt er vanaf. Het IP-adres van uw computer is voor uw internetaanbieder een persoonsgegeven. Uw internetaanbieder kan immers, zonder onevenredige inspanning, daarmee uw identiteit achterhalen. En dat kan hij omdat hij beschikt over de abonneegegevens die bij het IP-adres horen. U wordt voor hem geïdentificeerd door het IP-adres van uw computer.

Dat kan anders zijn als anderen, uw kinderen, gezinsleden of uw huisgenoten, gebruik maken van uw internetaansluiting. Het onwaarschijnlijk dat uw internetaanbieder, of iemand anders, in staat is de identiteit te achterhalen van die andere gebruikers. En dan zijn de IP-adressen, ook voor uw internetaanbieder, niet zonder meer persoonsgegevens. Ook uw internetaanbieder kan met de abonneegegevens de gebruikers niet identificeren. Hetzelfde doet zich voor als u gebruik maakt van 'gratis internet' in de trein of de wachtruimtes van Schiphol.

IP-adressen zijn dus vaak persoonsgegevens. Maar vaak ook niet. Het hangt er vanaf.[12]

Deze opvatting over IP-adressen en persoonsgegevens was lang onomstreden, maar blijkt te veranderen. En daarbij spelen privacytoezichthouders een rol die we gerust spelbepalend kunnen noemen. Eerst onderkenden zij dat IP-adressen vaak wel, maar toch ook vaak niet, kwalificeren als persoonsgegevens. Inmiddels vinden zij echter dat IP-adressen *altijd* en *per definitie* als persoonsgegevens moeten worden aangemerkt, of in elk geval als zodanig moeten worden behandeld.

Dat is een belangrijke ontwikkeling. En het is daarom de moeite waard om daarbij stil te staan. En ik doe dat dan ook.

Aan het begin van deze eeuw publiceerde het Europese overlegorgaan van nationale privacytoezichthouders, de Werkgroep Artikel 29, een document over privacy op internet. Daarin zette de werkgroep uiteen dat veel IP-adressen voor internetaanbieders pas persoonsgegevens zijn als zij systematisch de datum, het tijdstip en de duur van gebruik van die IP-adressen vastleggen. Immers, met deze gegevens kunnen zij, zonder onevenredige inspanning, internetgebruikers identificeren.

De werkgroep tekende daarbij aan dat dit niet geldt voor anderen dan internetaanbieders. Weliswaar is het soms

mogelijk om het IP-adres in verband te brengen met andere gegevens. Maar dat doet er niet aan af dat het, volgens de werkgroep, 'niet in alle gevallen en niet voor alle internetpartijen' mogelijk is om de gebruikers te identificeren. Uitgaand van het redelijkheids- en het relativiteitsaspect, merkte de werkgroep dus IP-adressen vaak wél, maar toch ook vaak niet, aan als persoonsgegevens.[13]

Onze eigen nationale privacytoezichthouder, het College bescherming persoonsgegevens, kon zich daarin wel vinden. In dezelfde periode kwam het College met een persbericht met de veelzeggende titel 'Een IP-adres is niet altijd een persoonsgegeven'.[14]

In de jaren daarop blijken vooral auteursrechthebbenden in staat om, door tussenkomst van de rechter, bij internetaanbieders de abonneegegevens te achterhalen die horen bij de IP-adressen van de gebruikers waarvan wordt vermoed dat die zich bezig houden met het uploaden van auteursrechtelijke beschermde werken. Vervolgens konden deze auteursrechthebbenden deze gebruikers identificeren. In dergelijke gevallen is er, volgens een advies van de werkgroep uit 2007, wél sprake van persoonsgegevens.[15]

Nu is het natuurlijk de vraag of het voeren van een gerechtelijke procedure geen onevenredige inspanning zou vergen. Niettemin is duidelijk dat de werkgroep onderkende dat IP-adressen, gelet op het redelijkheidsaspect, niet altijd persoonsgegevens zijn. In dat verband noemde de werkgroep ook het internetcafé. Daar is het vaak niet mogelijk om de identiteit van de gebruikers te achterhalen.[16]

Tot zover niets aan de hand. Maar dan komt de werkgroep, *nota bene* in hetzelfde advies, met heel nieuwe inzichten. Er is volgens de werkgroep al sprake van identificeerbaarheid als het gaat om gegevens waarvan het gebruik

(ik citeer):

> "*…rekening houdende met alle omstandigheden van het geval, naar verwachting gevolgen zal hebben voor iemands rechten of belangen.*

(en even verderop in hetzelfde advies vervolgt de werkgroep dan):

> *Het is voldoende als de persoon als gevolg van de verwerking van de betrokken gegevens anders wordt behandeld dan anderen.*"[17]

(einde citaat).

Voor de werkgroep gaat het ineens niet meer om het kunnen achterhalen van de identiteit van de betrokkene, maar of iemand kan worden ingedeeld 'aan de hand van sociaaleconomische, psychologische, filosofische of andere criteria'.[18]

> Voor de werkgroep gaat het daarbij bijvoorbeeld om de internetgebruikers die, omdat uit hun IP-adressen blijkt dat ze uit een bepaald land komen, geen toegang krijgen tot een bepaalde website of dienst. U heeft er zelf misschien ervaring mee als u in het buitenland een televisieprogramma wilt zien via Uitzending gemist. Dat lukt vaak niet. Op basis van het IP-adres wordt u dan anders behandeld dan andere gebruikers, en dat zonder dat uw identiteit bekend is.[19]

In deze opvatting over het persoonsgegevensbegrip gaat de werkgroep derhalve voorbij aan wat ik het identiteitsaspect noemde. En, anders dan soms wel wordt gesuggereerd,[20] betekent dat een radicaal andere invulling van het begrip.

In hetzelfde advies blijkt de werkgroep ook de betekenis van het redelijkheidsaspect vergaand te beperken. Als het gaat om internetcafés vindt de werkgroep dat IP-adressen toch wél als persoonsgegevens moeten worden behandeld. Weliswaar zijn internetgebruikers daar niet zonder onevenredige inspanning te identificeren. Echter, omdat het onduidelijk is

welke gebruikers wél of níet kunnen worden geïdentificeerd, moeten IP-adressen volgens de werkgroep toch altijd worden behandeld *alsof* het persoonsgegevens zijn. Voor de werkgroep is niet meer van belang of het een onevenredige inspanning kost om betrokkene te identificeren. Er is, zo stelde de werkgroep, alleen dan geen sprake van persoonsgegevens als het 'absoluut onmogelijk' is om iemands identiteit te achterhalen.
We zien hier dat de werkgroep voorbijgaat aan achtereenvolgens het identiteitsaspect én het redelijkheidsaspect. Een half jaar later zien we dat de werkgroep ook voorbij gaat aan het derde aspect, het relativiteitsaspect - het aspect dat erop ziet dat iets voor de één wel, en voor de ander niet, een persoonsgegeven kan zijn.

In een advies over internetzoekdiensten erkende de werkgroep dat IP-adressen 'in de meeste gevallen niet direct door zoekdiensten kunnen worden geïdentificeerd'. Maar daarbij merkte de werkgroep op 'dat identificatie [wel] door een derde worden [kan] worden verwezenlijkt'. Het gaat dan om rechtshandhavingsautoriteiten of auteursrechthebbenden. Omdat deze wél in staat worden geacht de identiteit van de gebruikers te achterhalen, vond de werkgroep dat zoekdiensten de IP-adressen toch moesten aanmerken als persoonsgegevens, óók als deze zoekdiensten zelf niet beschikken over de identificatiemogelijkheden.[21] Voor de werkgroep had dus ook het relativiteitsaspect geen betekenis meer.

Alles bij elkaar is duidelijk dat de werkgroep in deze adviezen, en ook in latere adviezen,[22] IP-adressen *hoe dan ook* als persoonsgegevens is gaan aanmerken. En dat is dan ook de conclusie die onze nationale privacytoezichthouder daaraan verbindt. In een persbericht over het zoekdienstenadvies stelde het College bescherming persoonsgegevens, zonder enige nuancering, dat nu 'ondubbelzinnig [is] vastgesteld dat IP-adressen persoonsgegevens vormen'.[23]

Er is dus veel veranderd in de opvattingen van toezichthouders over persoonsgegevens en IP-adressen. Voor dit voortschrijdend inzicht was aanvankelijk niet veel aandacht, wellicht omdat de adviezen van de werkgroep niet zo toegankelijk zijn - het is geen literatuur die iedereen voor zijn plezier leest. In de discussies over de nieuwe privacywet, de nieuwe privacyverordening, zien we echter dat dat de toezichthouders hun nieuwe opvattingen breed zijn gaan uitdragen.

De voorgestelde privacyverordening
In het voorstel voor de nieuwe privacyverordening wordt uitgegaan van een persoonsgegevensbegrip met dezelfde reikwijdte als waarmee we nu hebben te maken. In het voorstel gaat het nog steeds erom of iemand kan worden geïdentificeerd. En de middelen waarmee dat kan worden gedaan, moeten nog steeds 'redelijkerwijs in te zetten zijn'. Er wordt onderkend dat IP-adressen kunnen worden gebruikt om personen te identificeren. Maar volgens het voorstel betekent dat nadrukkelijk *niet* dat IP-adressen onder alle omstandigheden persoonsgegevens zijn.[24]

In de reacties op het voorstel zien we dat eerst een digitale-burgerrechtengroep zich daartegen afzet.[25] En later ook toezichthouders en vervolgens de politiek.[26] Hun standpunt is dat de verordening ook van toepassing zou moeten zijn als er gegevens worden verwerkt op basis waarvan de éne persoon van de andere kan worden onderscheiden. Het gaat hen niet meer om het *identificeren*, maar om het *individualiseren* – dat wil zeggen: onderscheid maken, of in goed Engels 'singling-out', je zou ook kunnen zeggen: isoleren.[27]

Een interessant accent daarbij is dat de werkgroep volhoudt dat identificeren ook individualiseren omvat, daarmee suggererend dat IP-adressen altijd al werden aangemerkt als persoonsgegevens - een standpunt dat in het licht van eerdere adviezen van de werkgroep onhoudbaar lijkt. Anderen dringen

gewoon aan op oprekking van het persoonsgegevensbegrip en erkennen dus dat identificeren niet hetzelfde is als het individualiseren.

Verwatering van de privacywet
Wat daarvan te vinden? Wat te vinden van het voorstel om het persoonsgegevensbegrip op te rekken? Het zal u inmiddels misschien niet verbazen dat ik dat ik daarbij bedenkingen heb.

Ik bespreek er vijf.

1. Begrenzing en afbakening. Een eerste bedenking betreft de drie aspecten die ik zo-even noemde.

In het opgerekte persoonsgegevensbegrip is het identiteitsaspect weg gedefinieerd. Aan het redelijkheids- en relativiteitsaspect wordt geen of beperkte betekenis toegekend. Het persoonsgegevensbegrip wordt daarmee minder contextafhankelijk en minder dynamisch. Op het eerste gezicht lijkt dat aantrekkelijk. De vraag of er sprake is van persoonsgegevens is dan gemakkelijk te beantwoorden. Er zal vrijwel altijd sprake zijn van persoonsgegevens. Althans, het zal niet uit te sluiten zijn dat er daarvan sprake is. Onbevredigende antwoorden als 'het hangt ervan af' en 'vaak wel, maar vaak ook niet' zijn dan verleden tijd.

Maar daartegenover staat dat de wet dan van toepassing zal zijn in veel situaties waarin dat onnodig is. Er moet dan, zo geven ook de voorstander van een opgerekt persoonsgegevensbegrip toe, worden voorzien in uitzonderingen. En, omdat we er niet zeker van zijn dat die in de wet zelf kunnen worden opgenomen, moet dan vaker een beroep worden gedaan op wat wel wordt genoemd 'een redelijke wetstoepassing' of een 'verstandige en flexibele toepassing'.[28]

Op zichzelf is dat niet nieuw. Ook de huidige privacywet schiet soms zijn doel ver voorbij. En de toezichthouder heeft dan ook al verschillende pogingen ondernomen om, met het instrument van 'de redelijke wetstoepassing', de werkingssfeer van de wet terug te brengen tot wat nog redelijk is. Deze pogingen hebben echter, behalve boeiende discussies, vooral veel rechtsonzekerheid opgeleverd.

> **Voorbeeld 1**. In de internetrichtsnoeren van december 2007 achtte het CBP het een redelijke wetstoepassing om pasfoto's en ander beeldmateriaal alleen dan aan te merken als rasgegevens in de zin van artikel 16 Wbp, als deze zijn gepubliceerd met het uitdrukkelijke doel om onderscheid te maken naar ras. In zijn arrest van 23 maart 2010, *LJN* BK6331, maakte de Hoge Raad daarmee korte metten.[29]
>
> **Voorbeeld 2**. In dezelfde internetrichtsnoeren worden criteria genoemd voor de uitzondering voor verwerkingen voor journalistieke doeleinden. Een jaar na de bekendmaking van de richtsnoeren blijken deze criteria al achterhaald door de uitspraak van het Hof van Justitie van 16 december 2008 in de Markkinapörssi-zaak.[30]
>
> **Voorbeeld 3**. In het voorjaar van 2009 kwam onze nationale toezichthouder met een beperkte uitleg van artikel 4, eerste lid, Wbp, dat gaat over de territoriale werkingssfeer van de wet. Een kleine twee jaar kwam de Art. 29 Werkgroep echter al met een opinie over deze kwestie. En daarin werd, niet geheel verrassend, een tegengesteld standpunt ingenomen.[31]

Van belang is dat de privacywet *sowieso* al veel open begrippen kent. Dat kan niet anders. Dit omdat de wet in veel uiteenlopende situaties van toepassing moet zijn. Echter, de wetgever had gedacht dat invulling van die open begrippen zou plaatsvinden in sectorale wetgeving, in de rechtspraak of door middel van zelfregulering.[32] Uit de evaluaties van de wet blijkt dat dit niet zo goed uit de verf is gekomen.[33] Alleen al om deze reden vind ik het onverstandig om in de volgende generatie van de privacywet uit te gaan van begrippen met nog minder onderscheidend vermogen.

Dat is mijn eerste bedenking tegen de oprekking van het persoonsgegevensbegrip.

2. Voorzienbaarheid. In het verlengde daarvan ligt een tweede bedenking. Deze betreft de voorzienbaarheid van de regels van de privacywet, dat wil zeggen: de 'foreseeability', zoals ontwikkeld in rechtspraak van het Europees Hof voor de Rechten van de Mens.

Een opgerekt persoonsgegevensbegrip betekent dat het voor de verantwoordelijken, en ook voor de betrokkenen, in veel gevallen onduidelijk wordt of de wet van toepassing is, en wat dat dan voor hen betekent. De werkingssfeer van de wet wordt onbepaald. Althans we kunnen niet goed bepalen wat de werkingssfeer is.

En dat maakt niet alleen de naleving maar ook de handhaving van die wet een hachelijke zaak. Om een regel te kunnen handhaven, en om vanwege de overtreding ervan een sanctie op te leggen, moet het de overtreder duidelijk kunnen zijn wat van hem wordt verwacht, welke normen er voor hem gelden. Een opgerekt persoonsgegevensbegrip maakt dat in veel gevallen moeilijk, zo niet: onmogelijk.[34]

3. Wat zijn de overwegingen? Een derde bedenking houdt verband met de overwegingen voor de oprekking van het persoonsgegevensbegrip. Of eigenlijk met het ontbreken daarvan.

Er gelden op dit moment al regels voor IP-adressen.[35] En er zijn wellicht redenen om meer regels daarvoor te stellen. En er zijn wellicht zelfs overwegingen waarom het persoonsgegevensbegrip moet worden opgerekt. Het geeft echter te denken dat dergelijke overwegingen niet of nauwelijks naar voren worden gebracht.[36]

> De overwegingen waarom het persoonsgegevensbegrip zou moeten worden opgerekt hebben weinig om het lijf. EP-rapporteur Albrecht volstaat met de 'justification' dat "*[t]he concept of personal data is further clarified with objective criteria. Identifiers that have a close relation to a natural person must be regarded as personal data.*"[37]
>
> De onderbouwing van de motie Elissen, waarin wordt verzocht om eenzelfde oprekking van het persoonsgegevenbegrip, beperkt zich tot de opmerking dat "*de definitie van persoonsgegevens de kern vormt van de nieuwe verordening en richtlijn […] en dat deze zorgvuldig tot stand zal moeten komen.*"[38]

De werkgroep beperkt zich tot verwijzingen naar een *selectie* van de eigen adviezen en het uitspreken van de wens dat toezichthouders toch iets te zeggen zouden moeten hebben over IP-adressen. Het zijn vooral doelredeneringen en autoriteitsargumenten, niet erg overtuigend. Het moet, zo zeggen de toezichthouders, omdat wij hebben gezegd dat het moet. En niet anders.[39]

Wat evenmin overtuigt is dat de overwegingen van de werkgroep grotendeels zijn gebaseerd op veronderstellingen. Een daarvan is dat de privacywet meer waarborgen zou bieden door eenvoudig de werkingssfeer ervan op te rekken. Is dat zo? Zou het echt zo eenvoudig zijn? Ik vraag het mij af. Er is misschien meer voor nodig. En dat zou, voordat we overgaan tot die oprekking, wel mogen worden opgehelderd.

4. Systeem van de wet. Een vierde bedenking betreft de uitgangspunten van de wet zelf.

De privacywet gaat zelf uit geïdentificeerde personen. Als er gebruik wordt gemaakt van inzagerechten, bijvoorbeeld, moet de verantwoordelijke zorg dragen voor een deugdelijke vaststelling van de identiteit van de inzagevrager.[40] Dat wordt lastig, om niet te zeggen: onmogelijk, als het gaat om gegevens over personen waarvan de identiteit onbekend is. Wat betekent in die situatie het inzagerecht nog?

En wat als het gaat om informeren van betrokkenen, één van de andere kernverplichtingen uit de wet..? Hoe moet dat als niet bekend is wie de betrokkenen zijn? Als u het weet mag u het zeggen. Niet nu, maar straks tijdens de receptie, wellicht.

5. Evaluaties. Een vijfde, voor dit moment laatste bedenking betreft de wetsevaluaties die ik al noemde.

Uit deze evaluaties kwam naar voren dat de onbepaaldheid van wettelijke begrippen wordt gezien als een groot knelpunt, misschien wel het grootste knelpunt van de wet. Het is ergerlijk dat er in de discussie over het persoonsgegevensbegrip geen aandacht is voor deze evaluaties.

Maar misschien trek ik mij dat te persoonlijk aan. U moet vooral niet denken dat ik deze evaluaties noem omdat ik, samen met andere eLaw-genoten, indertijd daaraan heb bijgedragen.[41]

Dat was een handvol bedenkingen. Er zijn er nog wel meer. Bijvoorbeeld met betrekking tot het subsidiariteitsvereiste[42] of de legitimering van de besluitvorming door toezichthouders. Maar u begrijpt het wel. Ik vind we er niet goed aan doen de werkingssfeer van privacywet zomaar op te rekken. Er is een serieus risico dat dit leidt tot verwatering van de privacywet, in die zin dat die wet dan op *alles* en *niets* van toepassing gaat zijn, en daarmee verwordt tot een wet zonder betekenis. Dat moeten we niet willen. En dat moet de wetgever niet willen.

En daarmee ben ik dan aangekomen bij de ambities van de privacywetgever.

De ambities van de privacywetgever

Als het gaat om privacy is de wetgever altijd al ambitieus geweest. De privacywetgever stelt regels voor veel, heel veel alledaagse en minder alledaagse, belangrijke en onbelangrijke, maatschappelijke, sociale en economische activiteiten. In de informatiemaatschappij heeft iedereen, niemand uitgezonderd, met de privacywet te maken. Is het niet als betrokkene over wie gegevens worden verwerkt, dan wel als verantwoordelijke die bepaalt op welke wijze dat gebeurt.

De privacywet gaat over burgerlijke vrijheden. Juist daarom moet er aandacht zijn voor de kwaliteit van de regels ervan. Van de privacywet mag, dat is mijn stelling, worden verwacht dat die een grote mate van begrijpelijkheid heeft, veel groter dan we bij andere wetten aanvaardbaar achten. In elk geval moet er, meer dan bij andere wetten, aandacht zijn voor de middelen waarmee de open begrippen ervan kunnen worden ingevuld.
Als het gaat om een wet waarmee per saldo maar een handvol te maken heeft, kan de wetgever het zich misschien veroorloven om minder gemakkelijk te begrijpen regels te stellen. Van degenen die het aangaat, en de toezichthouders en rechters die erover gaan, kan worden verwacht dat zij de moeite nemen om die regels te doorgronden. Van telecomaanbieders, bijvoorbeeld, mag worden verwacht dat ze zich verdiepen in de ondoorgrondelijkheden van telecomrechtelijke kostenoriëntatievereisten.[43] En als dat enige moeite kost is dat, gegeven het beperkte aantal telecomaanbieders en de hen beschikbare middelen, niet onoverkomelijk.[44]

Voor de privacywet is dat anders. De privacywet gaat ons allemaal aan. De privacywet moet daarom voor iedereen begrijpelijk *kunnen* zijn. De begrippen ervan moeten zonder onevenredige inspanning kunnen worden opgehelderd. Als er één wet géén 'wet voor specialisten' of 'superspecialisten' mag zijn, dan is dat de privacywet.[45]

De ambitie om het persoonsgegevensbegrip op te rekken staat daarmee op gespannen voet. De ambitie van de privacywetgever moet níet zijn om de werkingssfeer van de wet tot het oneindige op te rekken, maar om die wet begrijpelijk, werkbaar en uitvoerbaar te maken, naleefbaar en handhaafbaar. Want alleen dan kan de wet doen wat die moet doen, namelijk onze privacy beschermen.

Tot zover over de ambities van de privacywetgever.
Ik sluit af met een enkele opmerking over de rol van privacytoezichthouders.

En de rol van privacytoezichthouders
Over deze toezichthouders heb ik van alles gezegd. En er is zou bij u de indruk kunnen zijn ontstaan dat ik geen waardering hebt voor wat zij doen.

Die indruk is onjuist.

Het College Bescherming Persoonsgegevens, misschien wel één van de beste privacytoezichthouders die we in Nederland hebben, heeft zich de rol aangemeten om de privacywet nader in te vullen. Zo levert de toezichthouder een belangrijke bijdrage aan de rechtsvorming. En daarvoor past waardering.

Maar deze rechtsvormende rol stelt wel eisen. Een toezichthouder die geloofwaardig wil worden gevonden doet zijn best, of heeft er in elk geval geen moeite mee, om uit te leggen wat zijn overwegingen zijn. En precies dat ontbreekt in de discussie over persoonsgegevens en IP-adressen. Er is bij de toezichthouder schroom om toe te geven dat er bij hem sprake is van voortschrijdend inzicht. Er is bij hem terughoudendheid om toe te lichten waarom zijn opvattingen zijn veranderd.

Dat is ongelukkig. Daardoor wordt een zinvol gesprek onnodig bemoeilijkt en een serieuze discussie onmogelijk. Om deze rechtsvormende rol op een overtuigende wijze neer te zetten moet de toezichthouder het aandurven zijn opvattingen, en de ontwikkeling daarvan, te bespreken in bredere kring dan die van collega-toezichthouders en andere gelijkgezinden.

Privacy is van ons allemaal. De discussie daarover gaat iedereen aan. Voor wie om privacy geeft is dat vanzelfsprekend. Althans zou dat moeten zijn.[46]

Slotwoord
Zeer gewaardeerde toehoorders! Ik ben aangekomen bij mijn slotwoord. Het is gebruikelijk maar niet voorgeschreven, zo zegt de instructie, dat de hoogleraar aan het einde van de rede een dankwoord uitspreekt. Ik doe dat graag.

Voor het vertrouwen dat zij in mij stellen dank ik het College van Bestuur en het Bestuur van de Faculteit, in het bijzonder de rector, Carel Stolker, en de decaan, Rick Lawson, en alle anderen die hebben bijgedragen aan de totstandkoming van mijn benoeming.

Ik treed in de voetsporen van Hans Franken en Aernout Schmidt. Vanaf mijn eerste onzekere stappen in de academische wereld zijn zij mijn grote, en vaak onnavolgbare voorbeelden geweest. En dat zijn zij nog steeds. Hans, Aernout, heel veel dank daarvoor.

Ik ben ook dank verschuldigd aan de andere eLaw-genoten. Ik doe velen tekort, het is niet anders, door hier maar enkelen van hen te noemen. In willekeurige volgorde zijn dat: Bart, Bibi, Franke, Jaap, Jan-Jaap, Martijn, Rob, Tess, Wouter en natuurlijk Simone, met wie ik de leerstoel deel.

Het valt niet altijd mee om een voor iedereen aanvaardbaar evenwicht te vinden tussen mijn advocatuurlijke en academische bezigheden. Ik ben mijn kantoorgenoten bij Bird & Bird dankbaar dat ze mij, inmiddels meer dan 12 jaar, de ruimte geven om beide te kunnen doen. Ik doe ook hier velen tekort door maar twee *birds* te noemen. Dat zijn Marjolein Geus en Ella Meijaard, omdat beiden ieder op eigen wijze bepalend zijn voor mijn welbevinden op kantoor.

Ik zie met genoegen in het publiek ook studenten van het keuzevak telecomrecht en het keuzevak internetrecht. Ik zie ernaar uit om met u te verder verkennen wat kan en wat mag en wat moet mogen in de informatiemaatschappij. Er is, veel meer dan u zich misschien bewust ben, een grote behoefte aan juristen met specifieke kennis daarover.

Vanzelfsprekend gaat mijn dank, en niet in de laatste plaats, ook uit naar mijn familie. En dan allereerst naar degenen die hier vooraan zitten. Om redenen verband houdend met de bescherming van hun en mijn privacy treed ik daarover niet in detail, althans niet vanaf deze kansel.

Querida Geidy, por razones de privacidad no puedo explicarlo ahora, pero sabes que estoy muy feliz de que estés aqui, porque eres la persona mas importante para mi.

Ik heb gezegd.

Noten

1 F. Kuitenbrouwer, 'Wie geeft er nog om privacy?', *NRC Handelsblad* 15 september 2007, opgenomen in: F. Kuitenbrouwer, *Recht en vrijheid*, Uitgeverij NRC-boeken 2010, p. 141-143.

2 L. Mommers & G-J. Zwenne, 'Privacywetgeving is zelf het probleem', *Financieel dagblad*, 31 mei 2007, te vinden op <zwenneblog>.

3 Ik duid deze wetgeving aan als 'de privacywet' of 'de privacywetgeving'. De termen zijn misschien niet helemaal juist, maar wel ingeburgerd en in mijn ervaring voor vrijwel iedereen zonder toelichting begrijpelijk.

4 Art. 2, onder a, van Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *PbEG* L 281, 23/11/1995 p. 31-50.

5 Overw. 26 Richtlijn 95/46/EG.

6 *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 48-49, nr. 13, p. 2.

7 Zie J. Holvast, *Persoonsgegevens of niet: dat is de vraag*, Samsom Bedrijfsinformatie bv, Alphen aan den Rijn/Diegem 1996, p. 3-103; G. Overkleeft-Verburg, *De Wet persoonsregistraties* (diss. Tilburg), Deventer: Kluwer 1995, p. 524-541; zie verder ook onder andere: Van Esch, *Juridische aspecten van elektronische handel*, tweede herziene druk, Deventer 2007, p. 75 en 76; zie verder bijvoorbeeld ook K. Koelman & l. Bygrave, *Privacy, Data Protection and Copyrigh,* Amsterdam 1998; T. Oudejans, 'Internet on line. Privacy off-site', *Privacy & Informatie* 1998/4, p. 153-160; R. van Esch & P. Blok, 'Privacy en elektronische handel via internet', in J.M.A. Berkvens & J.E.J. Prins. *Privacyregulering in theorie en praktijk*, Deventer 2007, p. 205-206; T. Wisman & M. van der Linden-Smith, 'My secret life as an average person', *Tijdschrift voor Internetrecht* 2008, nr. 4, p. 88. Een afwijkend standpunt wordt igenomen door H.R. Kranenborg & L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees perspectief*, Deventer 2011, p. 64-65.

8 Dat een nummer of code, en soms zelfs een naam, op zichzelf nog niet maar in combinatie met andere gegevens wel, iemand kan identificeren, wordt in uiteenlopende rechtspraak zonder veel toelichting bevestigd. Zie bijv. HvJ 6 november 2003, zaak C-101/2001 (Lindqvist), overw. 24: "*Het […] begrip persoonsgegevens omvat volgens de definitie in artikel 2, sub a, daarvan [van de richtlijn 95/46/EG] iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Hieronder valt vanzelfsprekend iemands naam tezamen met zijn telefoonnummer of gegevens over zijn werksituatie en zijn liefhebberijen*"; HvJ 24 november 2011, zaak C-70/10 (Scarlet/Sabam), r.o. 51, waarin wordt vastgesteld dat als persoonsgegevens zijn aan te merken de IP-adressen "*die de precieze identificatie van die gebruikers mogelijk maken*" ("*those [IP-] addresses are protected personal data because they allow those users to be precisely identified*"); HR 4 september 2012, *LJN* BX4153: "*Een verdachte die is gedagvaard onder het voor haar (unieke) nummer 'NN.PL. 133C.V.71030.1000' wordt aangemerkt als een anonieme, d.w.z. ongeïdentificeerde verdachte. Zo een verdachte moet […] moet door de rechter worden geïdentificeerd door te vragen naar naam, voornamen, geboorteplaats, geboortedatum, gba-adres en feitelijk adres. Als er niettemin twijfel is over de identiteit van de verdachte is de rechter bevoegd nader onderzoek te laten doen omtrent de identiteit van de verdachte bestaande uit het afnemen van en vergelijken van vingerafdrukken en uit onderzoek van een identiteitsbewijs*" (0nderstrepingen toegevoegd). Zie over het begrip identificeren ook *Kamerstukken II* 1991/92, 22 694, nr. 3, p. 3.

9 *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 47.

10 Overkleeft-Verburg spreekt van het 'relativiteitsaspect van de herleidbaarheidstoetsing', zie G. Overkleeft-Verburg, *De Wet persoonsregistraties* (diss. Tilburg), Deventer 1995, p. 526-527, 534 en voetnoot 1836.

11 Onder verwijzing naar RFP760 (January 1980) wordt een internet address (IP-address) wel omschreven als "a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication."

12 Een in het voorjaar van 2011 gepubliceerd onderzoek naar rechtspraak in Europa over de kwalificatie van IP-adressen als persoonsgegevens levert een gevarieerd beeld

op. In het merendeel (84%) van de in het onderzoek betrokken uitspraken worden IP-adressen, gegeven de omstandigheden van het desbetreffende geval, aangemerkt als persoonsgegevens. In het onderzoek worden echter nogal wat voorbehouden gemaakt en in elk geval voor zover het Nederland en de EU betreft is het onderzoek onvolledig en weinig accuraat. Om deze reden kunnen daaruit nauwelijks harde conclusies worden getrokken. Zie Time.lex, 'Study of case law on the circumstances in which IP addresses are considered personal data, D3. Funal report, 2 May 2011.

13 Werkgroep Art. 29, Werkdocument Privacy op internet, (WP37), 21 november 2000, p. 22.

14 CBP, 'Een IP adres is niet altijd een persoonsgegeven', 19 maart 2001, z2000-0340.

15 Werkgroep Art. 29, Advies 4/2007 over het begrip persoonsgegeven, (WP136), 20 juni 2007, p. 22.

16 Werkgroep Art. 29, Advies 4/2007 over het begrip persoonsgegeven, (WP136), 20 juni 2007, p. 22.

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

18 De redenering van de werkgroep lijkt te steunen op de gedachte dat 'gebruiker' en 'computer', evenals 'identiteit' en 'persoonlijkheid' kunnen worden vereenzelvigd. De werkgroep maakt daarbij een niet nader toegelicht onderscheid tussen 'identiteit in enge zin' en 'identiteit in ruime zin'. De werkgroep merkt op dat: "*[i]n computerbestanden waarin persoonsgegevens zijn opgenomen, […] aan de geregistreerde personen doorgaans een unieke identificatiecode [wordt] toegewezen om verwisseling van personen in het bestand te voorkomen. Op het worldwideweb is het met behulp van bewakingsinstrumenten voor het webverkeer eenvoudig om het gedrag van een machine te identificeren en daarmee ook van de gebruiker ervan. De persoonlijkheid van de betrokkene kan op deze wijze worden achterhaald, zodat bepaalde besluiten aan hem of haar kunnen worden toegeschreven. Zonder zelfs maar naar de naam en het adres van de persoon te vragen, kan de betrokkene worden ingedeeld aan de hand van sociaaleconomische, psychologische, filosofische of andere criteria en kunnen bepaalde beslissingen aan hem of haar worden toegeschreven, omdat het voor het contactpunt voor de persoon (de computer) niet langer nodig is zijn of haar identiteit in enge zin bekend te maken. Met andere woorden, de identificatie van een persoon vereist niet langer het vermogen zijn of haar naam te achterhalen. De definitie van "persoonsgegeven" weerspiegelt ook dit.*" Werkgroep Art. 29, Advies 4/2007 over het begrip persoonsgegeven, (WP136), 20 juni 2007, p. 14-15.

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

20 Bijv. in dit persbericht van eurocommissaris Reding: EU Data Protection: European Parliament's legal affairs committee backs uniform data protection rules, MEMO/13/233 Brussels, 19 March 2013.

21 Werkgroep Art. 29, Advies 1/2008 over gegevensbescherming en zoekmachines, (WP148), 4 april 2008, p. 9; idem: Werkgroep Art. 29, Advies 4/2007 over het begrip persoonsgegeven, (WP136), 20 juni 2007, p. 9 en 22.

22 Vgl. ook deze overweging een advies over geolocatiediensten: "*Het feit dat de eigenaar van het apparaat op dit moment in bepaalde gevallen niet kan worden geïdentificeerd zonder onredelijke inspanningen te doen, staat niet in de weg van de algemene conclusie dat de combinatie van een MAC-adres van een WiFi-toegangspunt en de berekende locatie van het toegangspunt moet worden behandeld als een persoonsgegeven.*" Werkgroep Art. 29, Advies 13/2011 over geolocatiediensten op slimme mobiele apparaten, (WP 185) 16 mei 2011, p. 12.

23 CBP Persbericht, 'Internetzoekmachines moeten privacy respecteren', 7 april 2008.

24 Overw. 24 van de voorgestelde verordening.

25 Bits of Freedom, Brief van 2 maart 2012 aan Leden van de Commissie Veiligheid en Justitie inzake de conceptverordening gegevensbescherming.

26 *Kamerstukken II* 2012/13, 32 671, nr. 31, p. 2 en 15; *Kamerstukken II* 2012/13, 32 671, nr. 37; *Kamerstukken II* 2012/13, 32 671, nr. 42, p. 5; *Kamerstukken I* 2011/12, 33 169, C, p. 21.

27 G-J. Zwenne. 'Over IP-adressen en persoonsgegevens, en het verschil tussen individualiseren en identificeren', *Tijdschrift voor Internetrecht* 2011/1, p. 4-9; G-J. Zwenne, 'Regulering van IP-adressen (en andere mogelijke identifiers)', *Tijdschrift voor Internetrecht* 2011/2, p. 40-43.

28 Hustinx zei het zo: "*[een discussie over de reikwijdte van begrippen] is de weg terug, want daarmee bouw je een enorm dogmatisch en praktisch probleem aan de voordeur. Elke keer weer discussies over de vraag 'is dit nu wel of niet een persoonsgegeven'. Ik ben een groot voorstander van een brede werkingssfeer die je dan wel verstandig en flexibel moet toepassen*". Zie J.E.J. Prins, 'Acht gesprekken over privacy en aanpalende belangen', in H. Franken e.a., *Zeven essays over informatietechnologie en recht*, Den Haag 2003, p. 69-73. Een echo daarvan horen we in advies van de werkgroep over persoonsgegevensbegrip, waar wordt betoogd dat "*[h]et beter [is] de interpretatie van de definitie van persoonsgegeven niet onnodig te beperken, maar in het oog te houden dat er aanzienlijke ruimte is voor een flexibele toepassing van de regels op dergelijke gegevens.*" Aanmerkelijk genuanceerder is de toezichthouder in het Verenigd Koninkrijk in een 'article-by-article analysis paper': "*There is clearly considerable debate about whether certain forms of information are personal data or not. This is particularly the case with individual-level but non-identifiable - or not obviously identifiable data - such as is found in a pseudonymised database. We prefer a wide definition of personal data, including pseudonymised data, provided the rules of data protection are applied realistically, for example security requirements but not subject access. If there is to be a narrower definition it is important that it does not exclude information from which an individual can be identified from its scope. However, it is important to be clear that a wide definition plus all the associated rules in full would not work in practice. This is a real issue in contexts as diverse as medical research and online content delivery.*" Information Commissioner, Proposed new EU General Data Protection Regulation: Article-by-article analysis paper, V1.0 12 February 2013, p. 6-7. Vgl. C. Cuipers & P. Marcelis, 'Oprekking van het concept persoonsgegevens: beperking van privacybescherming?' *Computerrecht* 2012/187.

29 Vgl. deze overweging in de Cbp-internetrichtsnoeren van 11 december 2007: "*Alleen als een verantwoordelijke foto's of ander beeldmateriaal publiceert met het uitdrukkelijke doel om onderscheid te maken naar ras, is bijzondere oplettendheid geboden. In dat geval acht het CBP het een redelijke wetstoepassing om het beeldmateriaal aan te merken als een bijzonder persoonsgegeven [d.w.z. rasgegeven].*" En deze overweging uit HR 23 maart 2010, *LJN* BK6331: "*Uit de wetgeschiedenis volgt dat niet alleen gegevens die direct het ras van een persoon betreffen, maar ook gegevens waaruit informatie over het ras van een persoon kan worden afgeleid, zoals een foto van een persoon, als "gevoelige" informatie moet worden aangemerkt, die door de Officier van Justitie slechts kan worden gevorderd op de voet van de art. 126nd en 126nf Sv, dus na daartoe door de rechter-commissaris verleende machtiging. De Rechtbank heeft dat terecht tot uitgangspunt genomen. Het middel berust op de opvatting dat in een geval als het onderhavige, waarin de vordering uitdrukkelijk ook betrekking had op foto's van personen, toepassing van genoemde bepalingen alleen in aanmerking komt indien met de vordering is beoogd de desbetreffende gevoelige informatie aan die foto's te ontlenen. Die opvatting is onjuist, zodat het middel faalt*". Daarover G-J. Zwenne & L. Mommers, 'Zijn foto's en beeldopnamen 'rasgegevens' in de zin van artikel 126nd Sv en artikel 18 Wbp?', *Privacy & Informatie* 2010/5, p. 237 - 247; alsmede CBP Richtsnoeren Identificatie en verificatie van persoonsgegevens: gebruik van 'kopietje paspoort' in de private sector, juli 2012, p. 13.

30 HvJ 16 december 2008 ("Markkinapörssi"); daarover de annotatie van De Vries in *Tijdschrift voor Internetrecht* 2009/1, p. 48-50.

31 E.M.L. Moerel, 'Back to basics: wanneer is de Wet bescherming persoonsgegevens van toepassing?', *Computerrecht* 2008/3, p. 81-91, M.A.H. Fontein-Bijnsdorp, 'Art. 4 Wbp revisited: enkele opmerkingen inzake de toepasselijkheid van de Wet bescherming persoonsgegevens', *Computerrecht* 2008/6, p. 285-289, E.M.L. Moerel, 'Art. 4 Wbp revisited; naschrift De nieuwe WP Opinie inzake Search Engines', *Computerrecht* 2008-6, p. 290-298; G.J. Zwenne & C. Erents, 'Reikwijdte Wbp: enige opmerkingen over de uitleg van artikel 4,

eerste lid, Wbp', *Privacy & Informatie* 2009/2, p. 60-67; C.M.K.C. Cuijpers, 'Toepasselijk privacyrecht in de wolk', *Computerrecht* 2011/65; Werkgroep Art. 29, Advies 8/2010 over toepasselijk recht (WP 179), 16 december 2010.

32 *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 6; *Handelingen I* 1999/2000, 34, p. 1605.

33 G. Overkleeft-Verburg, *De Wet persoonsregistraties* (diss. Tilburg), Deventer 1995; G-J. Zwenne e.a., Eerste fase evaluatie Wet bescherming persoonsgegevens, WODC 2007; H.B. Winter et al, *Wat niet weet, wat niet deert*, WODC 2008.

34 Vgl. de volgende, nog steeds actuele overweging van het Europees Hof voor de Rechten van de Mensen in het Sunday Times-arrest: "*a norm cannot be regarded as a 'law' unless it is formulated with sufficient precision to enable citizens to regulate his conduct: he must be able – if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail*" EHRM 26 april 1979, NJ 1980, 146, *NJCM-bulletin* 1979, p. 62-63.

35 Zie bijv. art. 11.2a, 11.5, 13.2a Tw.

36 Een zeldzaam voorbeeld van een korte meer inhoudelijke overweging om de verordening ook van toepassing te laten zijn op niet-identificeerbare gegevens ('non identifiable data') biedt een tekst ondertekend door '62 leading senior academics'. Daarin wordt evenwel niet betoogd dat het persoonsgegevensbegrip moet worden opgerekt, maar dat de verordening ook van toepassing zou moeten zijn op andere dan persoonsgegevens. Zie S. Spiekermann et al, 'Data Protection in Europe: More than 60 Leading European Academics are taking a position', van 7 maart 2013 te vinden op http://dataprotectioneu.eu.

37 Jan Philipp Albrecht, Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Committee on Civil Liberties, Justice and Home Affairs (COM(2012)0011), Amend. 15, 28 en 84.

38 *Kamerstukken II* 2011/12, 32 761, nr. 37.

39 Werkgroep Art. 29, Advies 01/2012 over de voorstellen voor hervorming van het gegevensbeschermingskader, (WP191), van 23 maart 2012, p. 10-11.

40 Art. 37, tweede lid, Wbp; art. 15, vierde lid, van de voorgestelde verordening.

41 G-J. Zwenne e.a., Eerste fase evaluatie Wet bescherming persoonsgegevens, WODC 2007.

42 Overeenkomstig artikel 5 van Protocol 2 bij het Verdrag betreffende de Europese Unie wordt in par. 3.2 van de toelichting bij het voorstel wordt beknopt gemotiveerd waarom de verordening voldoet aan de in artikel 5, derde lid, van het verdrag gestelde subsidiariteits- en proportionaliteitsvereisten. De vraag is of die motivering, in het licht van de voorgestelde oprekking van het persoonsgegevensbegrip, nog voldoet. Vgl. *Kamerstukken I* 2011/12, 33 169, C, p. 18-19.

43 In zijn annotatie bij CBb 26 september 2012, *AB* 2013/22 beklaagt Stijnen zich erover dat "*[h]et veelvuldige gebruik van technisch en commercieel jargon en afkortingen deze uitspraak eigenlijk niet goed leesbaar [maakt] voor juristen die niet zijn gespecialiseerd in het telecommunicatierecht.*"

44 Schuyt noemt als voorbeelden de jagers en sportvisser die zich moeten verdiepen in de Flora en Faunawet (*Stb.* 1998, 402) C.J.M. Schuyt, *Op zoek naar het hart van de verzorgingsstaat*, Leiden/Antwerpen 1991, p. 215.

45 Zie bijv. *Kamerstukken II* 1991/92, 22 694, nr. 3, p. 3; *Kamerstukken II* 1997/98, 25 892, nr. 5, p. 6; E. Schreuders & H. Gardeniers, 'Materiële normen: de kloof tussen de juridische normen en de praktijk', *Privacy & Informatie* 2005/6, p. 260-262; G. Overkleeft-Verburg, *De Wet persoonsregistraties* (diss. Tilburg), Deventer 1995, p. 527; G-J. Zwenne e.a., Eerste fase evaluatie Wet bescherming persoonsgegevens, WODC 2007, p. 72-73, 116, 126.

46 Bart van der Velden, Bibi van den Berg, Laurens Mommers, Aernout Schmidt en Jos Webbink dank ik voor hun waardevolle opmerkingen op eerdere versies van deze tekst.

Prof.mr. Gerrit-Jan Zwenne

2011	hoogleraar recht en de informatiemaatschappij, Universiteit Leiden
2006	partner Bird&Bird LLP
2004-2011	universitair hoofddocent elaw@ Leiden, het centrum voor recht en in de informatiemaatschappij van de Faculteit der Rechtsgeleerdheid van de Universiteit Leiden
1992-1998	assistent in opleiding en universitair docent Recht & Informatica, Universiteit Leiden
1986-1992	doctoraal rechtsgeleerdheid, Rijksuniversiteit Leiden

Per 1 oktober 2011 is Gerrit-Jan Zwenne benoemd tot hoogleraar recht in de informatiemaatschappij bij eLaw@ Leiden, het centrum voor recht in de informatiemaatschappij van de Faculteit voor Rechtsgeleerdheid van de Universiteit Leiden. Hij houdt zich bezig met de toepassing en werking van internet-, telecom- en privacyregelgeving.

Daarvoor was Gerrit-Jan Zwenne al als universitair docent en universitair hoofddocent aan eLaw@Leiden verbonden. Hij studeerde rechten in Leiden en promoveerde in 1998 aan dezelfde universiteit op een proefschrift over belastingheffing en informatieverplichtingen. Hij verzorgt geregeld colleges en cursussen binnen zijn expertisegebieden en publiceert daarover. Naast zijn aanstelling bij eLaw@Leiden is hij advocaat bij Bird & Bird LLP te Den Haag.

In zijn oratie gaat Zwenne in op discussie over de privacywet en de toepassing daarvan op internet, en vooral of en in hoeverre de privacywet van toepassing is op IP-adressen en andere online identifiers. Daarbij bespreekt hij de ambities van privacywetgevers en de rol van privacytoezichthouders in de informatiemaatschappij. Hij stelt dat de wetgever niet de ambitie moet hebben om de werkingssfeer van de privacywet op te rekken tot het oneindige en verder. De privacywet moet begrijpelijk, werkbaar en uitvoerbaar gemaakt worden, en daarmee naleefbaar en handhaafbaar. De privacytoezichthouders spelen daarbij een belangrijke rol. Daarom mag van hen worden verwacht dat ze de moeite nemen om toe te lichten waarom ze de wet uitleggen, zoals ze die uitleggen.

Universiteit
Leiden