

# Niemand als consument

## *Naar een evenwichtig grondrecht op anonimiteit*

Lodewijk Asscher

Odysseus beweerde tegen de cycloop dat hij Niemand heette, en stak hem vervolgens in zijn oog. Was hij nu het schoolvoorbeeld van de onschuldige burger die zich alleen kon redden door anoniem te blijven of was zijn laffe daad de voorloper van de *cyberattack*? De consument heet allang niet meer alleen voor wie hij liefheeft.<sup>1</sup> Anno 2000 ziet hij zijn naam veranderen in een keten: zodra hij van een van de nieuwe ICT toepassingen gebruik maakt, ontstaat een spoor van gegevens, van informatie die van hem een exact profiel achterlaat, overal waar hij gaat.

### 1. Inleiding

Een van de cruciale aspecten van de zich ontwikkelende elektronische economie is het vertrouwen van de consument. Een werkelijke toename van de elektronische handel zal pas tot stand komen als de consument voldoende vertrouwen heeft in de nieuwe media. Veiligheid en privacy zijn sleutelbegrippen in de ontwikkeling van nieuwe diensten en markten. Soms kan veiligheid het beste bereikt worden door anonimiteit. Aan de andere kant wordt vaak het bezwaar geopperd dat anonimiteit een vrijbrief is voor cybermisdaad.<sup>2</sup> In deze bijdrage geef ik een korte schets van de grondrechten die de ICT consument beschermen bij het deelnemen aan het elektronisch verkeer. De bijdrage zal zich in het bijzonder richten op de vraag of de consument recht heeft op anonimiteit dan wel pseudonimiteit wanneer hij zich op de elektronische snelweg begeeft. Onder anonimiteit versta ik hier dat in het geheel geen naam bekend is. De consument hoeft zich op geen enkele manier te identificeren en gaat naamloos door *cyberspace*. Een eveneens voorkomend verschijnsel is dat gebruik wordt gemaakt van pseudonimiteit. Daarbij gebruikt de consument een aangenomen naam waarvan niet valt vast te stellen of dat zijn echte naam is. Net als in *de Nota Wetgeving voor de Elektronische Snelweg* worden beide begrippen naast elkaar gebruikt.<sup>3</sup> Daarnaast wordt een onderscheid gemaakt tussen de verschillende diensten die de consument afneemt, te weten: downloaden, surfen, email, semi-openbare informatiediensten als newsgroups en de overeenkomst op afstand.

### 2. Informatiegrondrechten

Wat zijn nu de relevante grondrechten die met anonimiteit te maken hebben? Ten eerste is het recht op privacy een relevant grondrecht, daar dat recht met name de integriteit en identiteit van het individu beschermt. Ook moet worden gedacht aan communicatievrijheid omdat voor vrije communicatie het geheim blijven van de identiteit van de deelnemers soms van belang kan zijn. Het gaat dan zowel om de vrijheid tot openbare communicatie als die tot niet-openbare communicatie. Het eerste

<sup>1</sup> Vergelijk Neeltje Maria Min, *Voor wie ik liefheb wil ik heten*, Amsterdam: Bert Bakker, 1996.

<sup>2</sup> Het gevaar van te sterke anonimiteit wordt ook benadrukt in het 'cybercrimerapport' van de Amerikaanse overheid; Working Group on Unlawful Conduct on the Internet, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of Internet*, Maart 2000, [www.cybercrime.gov/unlawful.htm](http://www.cybercrime.gov/unlawful.htm).

<sup>3</sup> *Kamerstukken II 1997/98*, 25 880, nr. 1-2.

wordt beschermd door de vrijheid van meningsuiting, het tweede door het communicatiegeheim.<sup>4</sup>

## 2.1 Openbare communicatievrijheid

Het recht op openbare communicatievrijheid omvat het recht op vrije meningsuiting, op toegang tot communicatiemiddelen en tot schaarse natuurlijke hulpbronnen en het recht informatie te ontvangen, alsmede het recht meningen te koesteren. Het recht op vrijheid van meningsuiting vindt in Nederland onder meer bescherming in artikel 7 van de Grondwet en in artikel 10 van het Europees Verdrag voor de Rechten van de Mens. Dat laatste artikel beschermt ook de andere fasen van het openbare communicatieproces. Of uit dit grondrecht een recht op anonimiteit kan worden afgeleid is niet zeker.

In de Verenigde Staten is het recht om anoniem te spreken onder de bescherming van het *First Amendment* gebracht. In de zaak *McIntyre v. Ohio* bepaalde het Amerikaanse Supreme Court dat een ieder het recht heeft anoniem te spreken.<sup>5</sup> Het Hoogerechtshof noemt een aantal mogelijke redenen die iemand kan hebben om te kiezen voor anonimiteit zoals angst voor economische repressie, zorgen over sociale gevolgen en de wens zoveel mogelijk privacy te behouden. De reden maakt echter uiteindelijk niet uit: *'whatever the motivation may be, at least in the field of literary endeavor, the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry'*. De beslissing van een auteur om anoniem te blijven vormt een aspect van de vrijheid van meningsuiting, zoals alle andere beslissingen die raken aan de inhoud van een publicatie. *McIntyre v. Ohio* gaat echter over een politieke zaak, waar de bescherming van de vrijheid van meningsuiting op zijn sterkst is. Het *Supreme Court* trekt dan ook de vergelijking met het recht op *secret ballot*, geheime stemming. Het is dus niet helemaal zeker of deze uitspraak voor alle vormen van anoniem communiceren zal blijken te gelden. Toch noemt het Hoogerechtshof in zijn conclusie het anoniem pamfletteren nog eventjes *'an honorable tradition of advocacy and of dissent'* want: *'Anonymity is a shield from the tyranny of the majority.'*

Voor de kwestie van anonimiteit en ICT is de tweede motivering van het Hoogerechtshof interessant. Immers, het wezenlijke doel van het *First Amendment* is: *'To protect unpopular individuals from retaliation – and their ideas from suppression at the hand of intolerant society.'* Dat belang bestaat ook in het ICT tijdperk. Analoog interpreterend kan gesteld worden dat juist ook de vrees voor repercussie en het daaruit voortvloeiende *chilling effect* een rol kunnen spelen op Internet. Ik denk hier vooral aan de gedachteswisselingen die plaatsvinden in de semi-openbare communicatievormen als newsgroups. Nu deze voor een ieder toegankelijk zijn en zelfs, dankzij nieuwe diensten, doorzoekbaar met zoekmachines, kan het voor de deelnemer aan dergelijke communicatie van groot belang zijn om zijn anonimiteit te bewaren. In Nederland werd een anonimiteitsverbod door de Hoge Raad in het

---

<sup>4</sup> L.F. Asscher, *Constitutionele convergentie van pers, omroep en telecommunicatie*, Deventer: Kluwer 1999, p. 9-16; E.J. Dommering e.a., *Informatierecht. Fundamentele rechten voor de informatiesamenleving*, Amsterdam: Cramwinckel 2000, p. 43-49.

<sup>5</sup> *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995).

*Muurkrantenarrest* niet in strijd met artikel 7 Grondwet geacht ondanks de nuttige functie van anonieme uitingen in de rechtsstaat.<sup>6</sup>

## 2.2. Communicatiegeheim

Het communicatiegeheim heeft grondslagen zowel in het recht op privacy als in het recht op communicatievrijheid. De privacygrondslag komt voort uit het privé-karakter van de niet openbaar gevoerde conversaties. De uitingsvrijheid is in het geding omdat de vrije uitwisseling van gedachten gevaar loopt als de communicatiekanalen gecorrumpeerd raken. Het kritisch uitlaten over politieke tegenstanders komt in het nauw als gesprekken worden afgeluisterd.

In Nederland wordt het communicatiegeheim beschermd door onder andere artikel 13 Grondwet en artikel 8 EVRM. In geen van beide artikelen is een directe bescherming van anonimiteit of pseudonimiteit opgenomen.

Wel is inmiddels in de jurisprudentie van het EHRM een lijn waarneembaar om ook bescherming te verlenen aan de transactiegegevens die ontstaan bij het transport van informatie. Deze zogenaamde verkeersgegevens omvatten de duur van een gesprek, maar ook de identiteit van de deelnemers. In het arrest *Malone* kan als visie van het EHRM worden gelezen dat een aanbieder van een telecommunicatiedienst de identiteitsgegevens van zijn klanten niet zonder meer aan derden of aan justitie mag afstaan. Artikel 13 Grondwet besteedt geen aandacht aan de bescherming van verkeersgegevens en is daarnaast wat ICT betreft beperkt tot de telefoon en de telegraaf in artikel 13 lid 2 Grondwet. De bescherming van *correspondence* in artikel 8 EVRM is daarentegen uitgebreid tot telefonie, en zal, naar valt te verwachten, ook tot andere vormen van privé-communicatie worden uitgebreid.<sup>7</sup> De opsomming van 13 Grondwet moet volgens sommige schrijvers niet worden gezien als limitatief maar als enumeratief zodat ook andere, modernere communicatiemiddelen eronder kunnen worden gebracht.<sup>8</sup> Door de meeste schrijvers wordt het huidige object van artikel 13 Grondwet echter als te beperkt beschouwd.<sup>9</sup>

## 2.3. Privacy

Het recht op privacy verzekert de bescherming van de persoonlijke levenssfeer. De precieze betekenis van het begrip staat echter niet vast. De inhoud van het algemene privacy artikel, artikel 10 Grondwet is dan ook tamelijk abstract.<sup>10</sup> De vraag of er een recht op anonimiteit c.q. pseudonimiteit onder kan worden begrepen valt niet met zekerheid te beantwoorden. De belangrijkste uitvoeringswet met betrekking tot de

<sup>6</sup> HR 24 juni 1980, *NJ* 1981, 659; J.M. de Meij e.a., *Uitingsvrijheid. De vrije informatiestroom in grondwettelijk perspectief*, Amsterdam: Cramwinckel 2000, p. 120-122.

<sup>7</sup> EHRM 2 augustus 1984 (*Malone*), *NJ* 1988, 534; EHRM 24 april 1990 (*Kruslin en Huvig*), *NJ* 1991, 52; J.A. Hofman, *Vertrouwelijke communicatie. Een rechtsvergelijkende studie over geheimhouding van communicatie in grondrechtelijk perspectief naar internationaal, Nederlands en Duits recht*, Zwolle: W.E.J. Tjeenk Willink 1995, p. 69-72. EHRM 6 september 1978, *AA* 1979, p. 327-334 (*Klass*).

<sup>8</sup> D.H.M. Meuwissen, *Grondrechten*, Utrecht: Spectrum, 1984, p. 178-179.

<sup>9</sup> Voor een overzicht zie Hofman 1995, p. 105-149; Dommering e.a. 2000, p. 71-86.

<sup>10</sup> Dommering e.a. 2000, p. 89; Natuurlijk kan in anonimiteit en pseudonimiteit ook een bedreiging van de privacy worden gezien of een bedreiging van de ontwikkeling van de elektronische handel. Immers zonder mogelijkheden van betrouwbare identificatie zal de ontwikkeling van bepaalde diensten op zich laten wachten en bestaat het gevaar van fraude waarbij iemand zich uitgeeft voor een ander of een anders pseudoniem.

informatieele privacy, de Wet Persoonsregistraties (WPR), neemt als uitgangspunt dat sprake moet zijn van een persoonsgegeven, dat wil zeggen een gegeven dat herleidbaar is tot een identificeerbare persoon of reeds geïdentificeerde persoon. In de opvolger van deze wet, de Wet Bescherming Persoonsgegevens (WBP), blijft dit uitgangspunt gehandhaafd.<sup>11</sup>

Aangezien er in hoofdstuk 8 van dit boek apart aandacht wordt besteed aan de algemene privacybescherming van de consument bij ICT zal ik in deze bijdrage niet ingaan op de exacte bepalingen van WPR en WBP. Grondbeginsel is echter dat – in welke situatie ook – de gegevensregistratie en het gebruik daarvan beperkt moeten blijven tot wat noodzakelijk en ter zake dienend is. De hoeveelheid verzamelde gegevens moet tot een minimum worden beperkt en het mag alleen gebeuren voor rechtmatige doeleinden.

Een kenmerk van de nieuwe netwerken en diensten (en in het bijzonder van Internet) is dat een enorme hoeveelheid (transactionele) gegevens wordt gegenereerd, waarmee de juiste verbindingen tot stand kunnen worden gebracht. Door de toenemende interactiviteit neemt die hoeveelheid verkeersgegevens alleen nog maar verder toe. Deze klikstroom zorgt per definitie voor een grotere hoeveelheid gegevens dan bij het passief consumeren van traditionele (*one way*) informatiediensten. ‘Via deze technieken kunnen “clicktrails” worden gecreëerd voor de Internetgebruikers. Clicktrails bevatten informatie over het gedrag van de gebruiker, zijn identiteit, de keuzes die hij heeft gemaakt en de links die hij heeft aangeklikt tijdens zijn bezoek aan een website. Ze worden opgeslagen op de webserver.’, aldus Aanbeveling 1/99.<sup>12</sup>

Hoewel deze verkeersgegevens in sommige landen en ook in de jurisprudentie van het EHRM<sup>13</sup> een zekere bescherming genieten in verband met de bescherming van het communicatiegeheim, blijft de enorme toename en de relatief grote toegankelijkheid van deze gegevens een probleem. Het spoor dat achterblijft neemt nog verder toe in omvang door het gebruik van *cookies* en *intelligent agents*. In dat verband is de recente klacht in de Verenigde Staten tegen reclamebedrijf Doubleclick bij de FTC van belang. Deze klacht, ingesteld door het EPIC (*electronic privacy information centre*) gaat met name over de beweerdelijke anonimiteit waar doubleclick voor zegt te zorgen terwijl ondertussen individuele profielen worden verkocht aan adverteerders.<sup>14</sup> Door ontwikkelingen op het gebied van *datamining* zijn steeds meer mogelijkheden ontstaan om de verschillende gegevens met elkaar in verband te brengen zodat ook hele nieuwe gebruikersprofielen kunnen worden vastgesteld over iemands persoonlijke voorkeuren.

De belangrijkste beginselen die gelden voor het gebruik en vervoer van informatie op het Internet of bij ICT in het algemeen vinden we in de artikelen 7, 10 en 13 Grondwet en 8 en 10 EVRM. Deze laatste artikelen maken op grond van artikel 6 van het EU-Verdrag ook min of meer deel uit van het gemeenschapsrecht. In dit verband

---

<sup>11</sup> Dommering e.a. 2000, hoofdstuk 5.

<sup>12</sup> Aanbeveling 1/99 van de Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens inzake de onzichtbare en automatische verwerking van persoonsgegevens op Internet door software en hardware, goedgekeurd 23 februari 1999, p. 5.

<sup>13</sup> EHRM 2 augustus 1984, *NJ* 1988, 534 (*Malone*).

<sup>14</sup> Klacht tegen Doubleclick bij de FTC, 10 februari 2000, [http://www.epic.org/privacy/internet/ftc/DCLK\\_comp\\_pr.html](http://www.epic.org/privacy/internet/ftc/DCLK_comp_pr.html).

is het belangwekkend dat de EU nu besloten heeft tot een Handvest voor de fundamentele rechten in de Europese Unie. Op dit moment is nog niet duidelijk welke status dat Handvest zal krijgen en of het Handvest nieuwe bepalingen zal bevatten die voor dit onderwerp relevant zijn.<sup>15</sup>

### 3. Grondrechten in de Informatiemaatschappij

Hierboven gaf ik reeds aan dat er kritiek bestaat op de huidige formulering van artikel 13 Grondwet. In Nederland woedt sinds 1997 een discussie over ‘Grondrechten in het digitale tijdperk’. In dat jaar werd een wijzigingsvoorstel inzake artikel 13 van de Grondwet voorgesteld waarover uitgebreid is gediscussieerd.<sup>16</sup> Kernpunten binnen die discussie waren de status en bescherming van verkeersgegevens, van onversleutelde email, en de vraag of er een notificatieplicht zou bestaan. Uiteindelijk trok de regering het voorstel in en benoemde een commissie Grondrechten in het digitale tijdperk.

De discussie moet dan uiteindelijk culmineren in een rapport van deze Commissie Franken, dat in mei 2000 zal verschijnen.<sup>17</sup> Daarna hoopt de regering nog tijdens Kok II een eerste lezing af te ronden van een wijzigingsvoorstel van de Grondwet. Het gaat vooral om de grondrechten op vrijheid van meningsuiting, op privacy en op het respecteren van het communicatiegeheim. Er is wel kritiek geuit op de opdracht aan de commissie, aangezien daarin werd opgeroepen tot aanpassing van de Grondwet aan de bestaande wetsvoorstellen en beleidsnotities. Daartoe behoort onder andere de reeds eerder aangehaalde Nota Wetgeving voor de Elektronische Snelweg met het beroemde adagium over *offline* en *online*.

#### 3.1. Offline ? Online

De regering heeft als uitgangspunt genomen dat wat *offline* geldt, ook *online* moet gelden.<sup>18</sup> Als beginsel kan dan gelden dat waar de gebruiker *offline* recht heeft op anonimiteit, hij dat ook *online* moet hebben. Dit blijkt uit de verklaring van Bonn, maar ook uit *de Nota Wetgeving voor de Elektronische Snelweg*.<sup>19</sup> Daarbij werd nadrukkelijk ook bedoeld op de grondrechten of fundamentele rechten. In de Nota geeft de regering ook aan dat juist waar het gaat om het garanderen van de fundamentele rechten een extra inspanning van de overheid verwacht mag worden. Hoewel de regering voor zich zelf vooral een ordenende rol ziet weggelegd in het informatietijdperk, moet zij sturend optreden om actief de bescherming van fundamentele rechten te waarborgen.<sup>20</sup>

Op dit *offline/online* dogma is wel het een en ander af te dingen. Zo zijn er in de *online* wereld per definitie meer monitormogelijkheden als gevolg van de

---

<sup>15</sup> Zie de site van het forum voor een Handvest van de Fundamentele Rechten in de Europese Unie: <http://db.consilium.eu.int/df/default.asp?lang=nl>.

<sup>16</sup> *Kamerstukken II*, 1997/98, 25 443; daarover: N.A.N.M. van Eijk, ‘(G)een recht op vertrouwelijke communicatie: fax en email vogelvrij’, *NJB* 1997, afl. 33, p. 1554-1555; E.J. Dommering, ‘Geen telefoongheim op de elektronische snelweg’, *Mediaforum* 1997-10, p. 142-147; A.J. Nieuwenhuis, ‘Vertrouwde en virtuele bescherming’, *NJCM-Bulletin* 4, 1998, p. 423-437.

<sup>17</sup> Besluit van 23 februari 1999, *Stb.* 1999, 101.

<sup>18</sup> *Kamerstukken II* 1997/98, 25 880, nr. 1-2, p. 5.

<sup>19</sup> Aanbeveling 97/3 p. 7.

<sup>20</sup> *Kamerstukken II* 1997/98, 25 880, nrs. 1-2, p. 13.

bovenbeschreven elektronische sporen die men achterlaat. Zowel het voortdurend aftappen als het onderzoeken welke krant iemand leest, is veel eenvoudiger in de *online* wereld dan in de *offline* wereld. De huidige wetgeving is nadrukkelijk afgestemd op de *offline* wereld en daarom niet automatisch geschikt voor online gebruik.<sup>21</sup>

### 3.2. Het democratisch evenwicht

Grondrechten zijn van oudsher een poging het machtsverschil tussen het individu en de staat te compenseren. Aangezien de staat het machtsmonopolie bezit moet de burger beschermd worden tegen willekeurige machtsuitoefening door de staat. In de informatiemaatschappij draait alles om kennis en moet de burger beschermd worden tegen verkeerd gebruik van die kennis. Bij de jurisprudentie met betrekking tot artikel 8 EVRM is reeds aan de orde gekomen dat pas effectieve bescherming mogelijk is als de burger op de hoogte is van de beperkingen op zijn grondrecht. Notificatie of kennisgeving van de over iemand verzamelde informatie is dan ook onontbeerlijk om de burger in staat te stellen de rechtmatigheid van de schendingen van zijn privacy aan de rechter voor te leggen. Het dogma van wat *offline* geldt moet ook *online* gelden kan hier te kort schieten. Immers, waar de consument *offline* vaak zelf maatregelen kan treffen om zijn anonimiteit en daarmee zijn privacy te waarborgen kan hij dat *online* niet zelf overzien. Natuurlijk staat hem een aantal technische hulpmiddelen ter beschikking maar de gedachtegang dat de verantwoordelijkheid geheel bij de consument moet liggen is niet juist. Daarom is de vaak gesuggereerde zelfregulering als oplossing van ieder probleem op het Internet ook onvoldoende. 'Uiteindelijk wordt het gebruik van persoonsgegevens op het web best geregeld door een combinatie van technologie, overheidsregulering, standaarden en andere vormen van zelfregulering'.<sup>22</sup> Bij zelfregulering is de kans groot dat de consument aan het kortste eind trekt. Hier ligt een belangrijke taak voor de overheid om actief de bescherming van de fundamentele rechten van haar onderdanen ter hand te nemen. Dommering wijst op de controleaspecten van nieuwe media: 'de bijzondere economische aspecten van netwerken en elektronische informatieverspreiding ... verschaften de Staat een uitstekende gelegenheid een vinger in de pan met pap te houden, die bij de drukpers zo bruut van het staatsformis was gehaald.' Inmiddels zitten de staat en zijn commerciële neefjes tot aan de ellebogen in de pap, en dreigt een doemscenario: het democratisch evenwicht is verstoord en de consument is het slachtoffer.<sup>23</sup>

### 4. Anonimiteit als oplossing

Een van de oplossingen voor dit probleem is om de herleidbaarheid tot het individu weg te nemen. Immers, door de zuivere toename van de hoeveelheid gegevens verschuift het evenwicht in de ICT naar meer controle en meer toezicht of dit nou door overheden of grote marktpartijen plaatsvindt. Dit vormt een verschuiving in het evenwicht die de vrijheid beknot. Anonimiteit zou dit evenwicht gedeeltelijk kunnen herstellen. Zodra anonimiteit wordt gegarandeerd kan een ieder deelnemen aan de Internetrevolutie zonder vrees voor registratie van elke beweging en zonder bang te zijn dat informatie wordt verzameld die later voor onaangename doeleinden kan

<sup>21</sup> S. Nouwt, *Privacyregels voor Internetberichten*, Deventer: Kluwer, 1999, p. 4-5.

<sup>22</sup> J. Dumortier, 'Privacybescherming en elektronische handel: wat na de richtlijn?', *Computerrecht*, 2000-1, p. 2-3.

<sup>23</sup> Dommering e.a. 2000, p. 492-498.

worden gebruikt. Ook in de traditionele ICT diensten werd altijd al de noodzaak van anonimiteit onder bepaalde omstandigheden erkend. De zogenaamde zelfhulp lijnen (kindertelefoon e.d.) vormen hiervan een sprekend voorbeeld.

Hoe zou meer anonimiteit er in de praktijk uitzien? Volgens Aanbeveling 97/3 moet worden gezocht naar aanknopingspunten met oudere diensten via oudere media. Dit houdt echter wel een gevaar in van simplificatie.<sup>24</sup> Hieronder volgt kort een bespreking van anonimiteit bij de diverse ICT diensten.

#### **4.1. Toegang tot (tele)communicatiediensten**

Traditioneel is de anonieme toegang tot telecommunicatiediensten altijd al gegarandeerd geweest. Immers, de wet schreef voor dat telefooncellen aanwezig moesten zijn, en dat daarbij betaald kon worden met muntgeld of met (anonieme) telefoonkaarten. De anonimiteit van een afnemer van een openbare telecommunicatiedienst vormt tevens het onderwerp van een aantal bijzondere regels in de Telecommunicatiewet. Zo zijn in hoofdstuk 11 regels opgenomen omtrent niet-gespecificeerde telefoonnota's en anonimiteit van abonnee tot dienstaanbieder door de plicht verkeersgegevens zo snel mogelijk te vernietigen of te anonimiseren. Daarnaast gelden bijzondere bepalingen met betrekking tot nummeridentificatie, CLI.<sup>25</sup> Bij de nieuwe mobiele diensten wordt een nieuw probleem gevormd door de onduidelijke status van locatie- of celidentiteitsgegevens. Ook hier kunnen echter telefoonkaarten soelaas bieden.<sup>26</sup>

Het ligt in de rede om ook op Internet de mogelijkheid van anonieme toegang uit te breiden.

#### **4.2. Surfen en bladeren op het Internet**

Waar in de wereld buiten de ICT het rondneuzen of *browsen* meestal anoniem kan en zal plaatsvinden<sup>27</sup>, is bij toepassing van ICT, en met name op het Internet, het surfen en bladeren een activiteit die sporen achterlaat die identificeerbaar zijn tot de consument. Dergelijke sporen bevatten voor commerciële sites een schat aan informatie die kan worden gebruikt voor *direct marketing* en voor verbetering van de reclamecampagnes in het algemeen. Er is echter geen zwaarwegend belang dat zich verzet tegen het anoniem surfen. Het verzamelen van persoonsgegevens bij het surfen moet dan ook volledig transparant gebeuren en behoeft de *informed consent* van de surfer. Zolang dat niet gebeurt, is de surfer geschaad in zijn recht op anonimiteit dat hier wordt beschermd door het recht op privacy en vrije meningsuiting. Dit houdt ook in dat van een reële *opt-out* clause sprake moet zijn. Dat wil zeggen dat de consument de registratie van zijn surfgegevens moet kunnen uitschakelen.

---

<sup>24</sup> L.F. Asscher 1997, 'E-mail een ansichtkaart?', *Mediaforum* 1997-7/8, p. 103.

<sup>25</sup> Dommering e.a. 2000, p. 428.

<sup>26</sup> G.N.M. Sciarone-Gorgels 'Hoofdstuk 11 van de Telecommunicatiewet rijp voor revisie?', in: *Privacy en Informatie*, 1999-5, p. 201.

<sup>27</sup> 'In het gewone maatschappelijke verkeer kunnen burgers zich in beginsel anoniem op de openbare weg bewegen. Het vragen naar de identiteit is voorbehouden aan personen die daartoe op grond van de wet zijn bevoegd.', *Kamerstukken II* 1997/98, 25 880, nrs. 1-2, p. 129.

Aanbeveling 1/99 neemt een scherp standpunt in over het automatisch vergaren van persoonsgegevens: Immers, 'een voorwaarde voor de rechtmatige verwerking van persoonsgegevens is dat de betrokkene hiervan op de hoogte wordt gesteld en er zich dus van bewust is dat deze verwerking plaatsvindt'. Volgens Aanbeveling 1/99 moeten de verzamelaars van persoonsgegevens betrokkenen ook de mogelijkheid bieden eenvoudig inzage te verkrijgen in de gegevens die over hem of haar zijn verzameld. Dit heeft aanmerkelijke gevolgen voor het gebruik van cookies en het automatisch meesturen van informatie bij het totstandkomen van verbinding. Belangrijkste aanbeveling is echter om providers de plicht op te leggen dat software zodanig geconfigureerd moet zijn dat slechts het strikt noodzakelijke minimum aantal persoonsgegevens wordt opgeslagen. Vervolgens moet er sprake zijn van een gebruiksvriendelijke optie waarbij de gebruiker kan aangeven of informatie mag worden doorgestuurd.<sup>28</sup>

Tijdens de parlementaire behandeling van voorstel 25 443 inzake de wijziging van artikel 13 Grondwet werd de vraag gesteld of surf- en zoekgedrag door de minister onder het begrip verkeersgegevens werd gerekend. Daarnaast werd gevraagd of dit reeds in de Telecommunicatiewet was geregeld en of dat dan niet alsnog zou moeten gebeuren.<sup>29</sup> De reactie van de minister was veelzeggend: '...dat zoekgedrag niet specifiek in de Telecommunicatiewet wordt geregeld. Verkeersgegevens betreffen slechts data, tijdstippen waarop de telecommunicatie plaatsvindt en de telefoonnummers waartussen die plaatsvindt en de verzonden hoeveelheid gegevens. Welke Internetsites zijn bezocht en welke pagina's zijn bezocht valt er niet onder. Dat onderscheid wordt hier gemaakt.'<sup>30</sup> Sommigen leiden hieruit af dat alleen gegevens die iets zeggen over beide deelnemers aan een communicatie de verzwaarde bescherming van verkeersgegevens zou toekomen. Immers, voor de 'gewone transactiegegevens' van het Internetgebruik geldt altijd nog de gewone privacybescherming. Surfgegevens zijn dan niet a priori gevoeliger dan gegevens die bij een bank over ons zijn opgeslagen.<sup>31</sup> Toch meen ik dat juist de hierboven beschreven verstoring van het evenwicht tussen privacy en openbaarheid op het Internet er toe moet leiden dat juist ook surfgegevens moeten genieten van de zware bescherming die ook ten deel valt aan verkeersgegevens in de zin van de Telecommunicatiewet. Dat zou betekenen dat ook artikel 11.5 Telecommunicatiewet onverkort van toepassing is op surfgegevens.<sup>32</sup> Dat artikel bepaalt dat verkeersgegevens na beëindiging van een oproep moeten worden verwijderd of geanonimiseerd. Hoewel er gerechtvaardigde uitzonderingen bestaan, bijvoorbeeld in geval dat nodig is om een rekening op te maken, mag er toch verlangd worden dat op Internet in ieder geval wordt overgegaan tot anonimisering van de betreffende gegevens conform artikel 11.5 Tw. Onder anonimisering moeten we volgens de Memorie van Toelichting verstaan dat de gegevens zodanig worden bewerkt dat deze redelijkerwijs niet meer herleidbaar zijn tot individuele personen. Dit kan betekenen dat de verplichting verder strekt dan slechts het verwijderen van de naamgegevens

---

<sup>28</sup> Aanbeveling 1/99 van de Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens inzake de onzichtbare en automatische verwerking van persoonsgegevens op Internet door software en hardware, goedgekeurd 23 februari 1999, p. 2-4.

<sup>29</sup> Sciarone-Gorgels 1999, p. 196-204.

<sup>30</sup> *Handelingen II*, 14 januari 1998, TK 41-3344-3358.

<sup>31</sup> Sciarone-Gorgels 1999, p. 199.

<sup>32</sup> Zie in die zin ook E.J. Dommering e.a., *Handboek Telecommunicatierecht. Inleiding tot het recht en de techniek van de telecommunicatie*, SDU, 1999, p. 620-622.

maar dat ook een inspanning verplicht is om te voorkomen dat gegevens tot een persoon herleidbaar blijven.<sup>33</sup>

### 4.3. Email

De consument die gebruik maakt van een e-maildienst is meestal identificeerbaar op grond van zijn email of IP-adres. Deze informatie is doorgaans beschikbaar voor zowel ontvanger als access provider alsmede dienstverleners die zich met het transport belasten.

Een emailbericht bevat de volgende onderdelen,

- a. de adresgegevens van geadresseerde, afzender of beiden, de zogenaamde *header*.
- b. het onderwerp, subject, een korte aanduiding van datgene waar het bericht over gaat en de berichttekst zelf. De header bevat ook informatie als tijdstip en datum van verzending en routeringsinformatie over de door het bericht afgelegde route.<sup>34</sup>

De voornaamste anonimiteitconstructies waarvan de consument gebruik zou kunnen maken zijn:

- a. de anonieme remailer. Dat wil zeggen dat de afzender zijn mail stuurt via een *remailer* die het anonimiseren als dienst aanbiedt.<sup>35</sup>
- b. anonieme toegang tot het Internet. De gebruiker begeeft zich anoniem op het Internet doordat hij tevoren prepaid Internettijd heeft ingekocht of doordat hij vanuit een openbaar Internetpunt belt (de zogenaamde openbare Internetkiosk, zie ook 4.1).

Bij mogelijkheid *a* is er onder omstandigheden de mogelijkheid de anonimiteit op te heffen bijvoorbeeld ten behoeve van een strafrechtelijk onderzoek. Dat biedt de mogelijkheid het recht op anonimiteit af te wegen tegen andere zwaarwegende belangen. Voor de betrokkenen vervult de *anonymous remailer* een vertrouwensfunctie, zijn systeem dient daarom duidelijk tegen inbraken beveiligd te zijn.<sup>36</sup>

In vergelijking is de klassieke post een veel beter geschikt middel om anoniem aan deel te nemen. Er is sprake van een systeem waarbij de afzender zich niet bekend hoeft te maken en waarbij een volledig geanonimiseerd betaalmiddel - de postzegel - wordt gehanteerd. Daarnaast kan de verzender van post ook voor de ontvanger van de post anoniem blijven. Mochten zwaarwegende belangen daartoe nopen, dan kan de anonimiteit met een rechterlijke last worden weggenomen.

Hoewel de minister volhield dat de inloggegevens uit de header van een emailbericht niet onder het begrip verkeersgegevens en daarmee niet onder het communicatiegeheim vielen, ben ik met Dommering e.a. van mening dat bij toepassing van het adrescriterium de header wel degelijk onder het communicatiegeheim gebracht kan worden. Volgens die redenering is de identiteit van de geadresseerde een integraal onderdeel van het geheim en mag daarom niet verder gebruikt worden dan voor het transport noodzakelijk is. Iets anders ligt het bij

<sup>33</sup> *Kamerstukken II* 1996/97, 25 533, nr. 3, p. 120.

<sup>34</sup> H.W.K. Kaspersen, A. Hofman, J. Verbeek, *Vertrouwelijkheid van e-mail*, Kluwer, Deventer, 1999, p. 97-98.

<sup>35</sup> Voor de technische aspecten van het remailen zie:  
<http://www.stack.nl/~galactus/remailers/index.html>

<sup>36</sup> Kaspersen/Hofman/Verbeek 1999, p. 103-104.

de loggegevens ter zake van openbare websites. Daar zou wellicht kunnen worden volstaan met de bescherming van gewone persoonsgegevens.<sup>37</sup>

Als meer algemene conclusie kan worden gesteld dat de mogelijkheden van anoniem emailgebruik thans nog tamelijk beperkt zijn.

#### **4.4. Nieuwsgroepen, chatboxen, bulletin boards**

Op het Internet is ook een aantal communicatievormen populair geworden die niet eenvoudig zijn in te delen volgens het oude schema van openbaar versus niet-openbaar. Het kan gaan om nieuwsgroepen of chatboxen waar gemeenschappelijke interesses op het programma staan. Het in zo'n groep plaatsen van mededelingen gebeurt in de wetenschap dat het ontvangend publiek onbepaald is en dat dus de mededelingen bij iedereen kunnen terechtkomen. Er is wel voorgesteld de deelname aan dergelijke groepen afhankelijk te stellen van identificeerbaarheid zodat onrechtmatige uitlatingen kunnen worden bestreden. Aanbeveling 97/3 vindt dat echter te ver gaan en maakt de vergelijking met prikborden in de offline wereld.<sup>38</sup> Mogelijke tussenoplossingen zijn hier de aanwezigheid van een moderator die bepaalde deelnemers de toegang tot de groep kan ontzeggen of de gebruikmaking van pseudonimiteit zodat de band met de echte identiteit kan worden hersteld als dat noodzakelijk is. De fundamentele rechten op privacy en vrije meningsuiting mogen dan ook niet verder worden beperkt dan noodzakelijk is. Nu er andere methoden voor handen zijn om het probleem van onrechtmatige uitlatingen hier aan te pakken, mag volledige identificeerbaarheid dus niet meer worden gevraagd. Mede met het oog op de vrijheid van meningsuiting is het van groot belang dat ook in de toekomst de mogelijkheid blijft bestaan anoniem aan dergelijke communicatievormen deel te nemen.

#### **4.5. Het kopen van goederen en diensten over het Internet**

Het kopen van goederen of diensten met behulp van ICT is de laatste jaren enorm in omvang toegenomen. Dit heeft mede geleid tot een aantal specifieke regelingen op het gebied van consument en ICT. Hier springen met name de Richtlijn overeenkomsten op afstand en de Ontwerprichtlijn e-commerce in het oog.<sup>39</sup> De vraag is of de consument identificeerbaar zou moeten zijn om deel te nemen aan handel met behulp van ICT.

Buiten de ICT is anoniem betalen de norm, zeker waar het gaat om kleine aankopen. Gaat het om koop op afbetaling, of grote bedragen, dan bestaat vaak een plicht tot identificatie. Het zou dan ook goed zijn als de consument ook op het Internet de keuze heeft uit verschillende betaalwijzen. De ontwikkeling van *ecash* is wat dat betreft buitengewoon belangrijk. Fundamentele voorwaarde voor de doorbraak van anoniem

---

<sup>37</sup> E.J. Dommering e.a., *Handboek Telecommunicatierecht. Inleiding tot het recht en de techniek van de telecommunicatie*, SDU 1999, p.620-621; Asscher 1999, p. 57-75; Dommering e.a. 2000, p. 72

<sup>38</sup> Aanbeveling 97/3, p. 9.

<sup>39</sup> Richtlijn 97/7/EG van het Europese Parlement en de Raad van 17 februari 1997 betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten, Pb. EG 4 juni 1997, nr. L 144/19; Gemeenschappelijk standpunt door de Raad vastgesteld met het oog op de aanneming van Richtlijn van het Europees Parlement en de Raad betreffende bepaalde juridische aspecten van de diensten in de informatiemaatschappij, met name de elektronische handel in de interne markt, 98/0325 COD, van 28 februari 2000.

ecash is dat de echtheid gegarandeerd kan worden. Dit vereist een aantal authenticeringmaatregelen. Aanbeveling 97/3 geeft aan dat bij anonieme *ecommerce* in sommige gevallen strijd kan ontstaan met de regels tegen het witwassen, in de meeste gevallen zal dit echter geen problemen opleveren.

## 5. Conclusie

In de discussie over anonimiteit en ICT bestaat de neiging tot zwart-wit denken. Het is echter niet nuttig de problematiek eendimensionaal – of digitaal – voor te stellen. Het gaat niet om hetzij helemaal privacy hetzij helemaal niet.<sup>40</sup> Hierboven gaf ik aan dat er slechts een indirect grondrecht op anonimiteit kan worden afgeleid uit de bestaande grondrechten. Een recht dat bovendien sterk afhankelijk is van de vraag welke dienst de consument afneemt. Ook is duidelijk dat de huidige grondrechten die stammen uit het ‘offline-tijdperk’ niet meer helemaal voldoen in het Internet tijdperk. Wat dat betreft is het hoopgevend dat de overheid duidelijk te kennen geeft een aanzet te willen geven aan hernieuwde formulering in het digitale tijdperk. Of het adagium ‘*wat offline geldt, moet online gelden*’ daarbij de meest geschikte leidraad is, valt te betwijfelen. Anonimiteit biedt een fraai voorbeeld van een recht dat als oplossing zou kunnen fungeren voor de problematiek van de steeds afnemende privacy op Internet. In de Nota Wetgeving voor de Elektronische Snelweg staat het als volgt: ‘De elektronische snelweg vergroot zowel de behoefte aan een meer persoonsgebonden identiteitsvaststelling, als een anoniem deelnemen aan het elektronisch verkeer. Daarbij blijft het huidige uitgangspunt...ongewijzigd...: voor zover de wet... niet noodzaakt tot opheffing van de identiteit, moet anonimiteit op de elektronische snelweg het uitgangspunt zijn.’<sup>41</sup>

Het is van het grootste belang voor de waarborging van de fundamentele rechten van burgers in het algemeen en consumenten in het bijzonder dat de consument van ICT de mogelijkheid heeft voor anonimiteit te kiezen. Actie is denkbaar op drie niveaus. Ten eerste moet in de regelgeving blijk worden gegeven van het feit dat anonimiteit een recht is en dat de verzameling van identificeerbare gegevens dus tot een minimum moet worden beperkt. Ten tweede moet worden nagedacht over technologische verbeteringen die anonimiteit in de praktijk dichterbij moeten brengen. Tenslotte moet gericht onderzoeksgeld worden ingezet om de mogelijkheid van anonieme toegang tot het Internet te bevorderen.<sup>42</sup> Ook moet worden gewerkt aan bewustwording van publiek en aanbieders van toegang, diensten en producten via ICT.

Voor de Nederlandse consument is het te hopen dat in de komende jaren door de diverse initiatieven rond grondrechtenbescherming zijn positie enigszins wordt versterkt. Belangrijk daarbij is dat in een nieuwe communicatieparagraaf de duidelijke ‘Internetrechten’ op anonimiteit en encryptie worden verankerd. Daarin kunnen dan met helder omschreven beperkingclausules de grenzen van een recht op anonimiteit worden aangegeven.

<sup>40</sup> Sciarone-Gorgels 1999, p. 200.

<sup>41</sup> *Kamerstukken II* 1997/98, 25 880, nrs. 1-2, p. 129; Het opheffen van identiteit moet hier vermoedelijk gelezen worden als het bekendmaken van identiteit of het opheffen van anonimiteit (LFA).

<sup>42</sup> Aanbeveling 97/3, p. 13.

L.F. Asscher<sup>?</sup>

---

<sup>?</sup> Mr L.F. Asscher is als projectonderzoeker verbonden aan het Instituut voor Informatierecht, Universiteit van Amsterdam.